EXTRICOM WLAN SYSTEM USER GUIDE

EXTRICOM MS-500/1000
EXTRICOM LS-3000
EXTRICOM RP-30n/40En/22n/32n/22En

Document Version v0.20

Copyright

No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Extricom Ltd. No patent liability is assumed with respect to the use of the information contained herein.

While every precaution has been taken in the preparation of this publication, Extricom Ltd. assumes no responsibility for errors or omissions. The information contained in this publication and features described herein are subject to change without notice. Extricom Ltd. reserves the right at any time and without notice, to make changes in the product.

Copyright © 2012 Extricom Ltd. All rights reserved. The products described herein are protected by U.S. Patents and may be protected by other foreign patents, or pending applications.

Important Notice:
Read this user manual, safety instructions, and the release notes for your switch firmware, before installing and operating the Extricom WLAN system.

Disclaimer

Extricom makes no representations or warranties whether expressed or implied, that the Extricom wireless local area network (WLAN) system or any component thereof shall meet the purchaser's operating requirements or that system operation will be uninterrupted or error-free. All WLANs, including the Extricom WLAN system, can potentially be affected by outside sources of interference such as other broadcasting devices, radiation, device immunity level, and other external sources of interference.

Extricom Extricom

! ***This equipment has been approved for mobile applications where the equipment is to be used at distances greater than 20cm from the human body (with the exception of hands, wrists, feet and ankles). Operation at distances of less than 20 cm is strictly prohibited.***

Changes or modification to equipment not expressly approved by Extricom Ltd. is strictly prohibited and could void the user's license to operate the equipment.

- ***Extricom access points are for indoor use only.***
- ***The maximum antenna gain is 4dBi***
- ***An Extricom access point includes multiple WLAN radio modules; each radio module is configured separately and serves a different set of clients. There is no relation between transmissions on different radio modules, hence:***
  - ***The same information cannot be transmitted over separate Radio modules.***
  - ***Radio modules cannot transmit simultaneously over the same radio channel.***
  - ***Client can transmit and receive data through one Radio module.***

! ***Please check the release notes for your version of Extricom firmware before installing or operating the system. The relevant release notes supersede this user guide.***

The availability of some specific channels and/or operational frequency bands is country-dependent and the firmware is programmed at the factory to match the intended destination. This firmware setting is not accessible by the end user.

Federal Communication Commission and Industry Canada Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC and IC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC & IC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference
2) This device must accept any interference received, including interference that may cause undesired operation.

Important Note:

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25 GHz band are restricted to indoor usage only, to reduce potential for harmful interference to co-channel satellite systems.

The maximum antenna gain permitted (for devices in the 5725-5825 MHz band) must comply with the EIRP limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

Sec. A9.2 (3): For the band 5725-5825 MHz, the maximum conducted output power shall not exceed 1.0 W or 17 + 10 log10 B, dBm, whichever power is less. The power spectral density shall not exceed 17 dBm in any 1.0 MHz band. The maximum EIRP shall not exceed 4.0 W or 23 + 10 log10 B, dBm, whichever power is less. B is the 99% emission bandwidth in MHz

Fixed point-to-point devices for this band are permitted up to 200 W EIRP by employing higher gain antennas, but not higher transmitter output powers. Point-to-multipoint systems, Omni-

directional applications and multiple co-located transmitters transmitting the same information are prohibited under this high EIRP category. However, remote stations of point-to-multipoint systems shall be permitted to operate at the point-to-point EIRP limit provided that the higher EIRP is achieved by employing higher gain directional antennas and not higher transmitter output powers.

Table of Contents

About This Guide **1**

Audience 1
Conventions 1
Safety Precautions 1

Chapter 1 Introduction to the Extricom Wireless LAN System **3**

Overview of the Extricom WLAN System 3
Features and Benefits 5
Overview of the Multi Series (MS) Switch Platform 9
Overview of the Extricom Access Points 11
Access Points with Internal Integrated Antennas 11
Access Points with Connectors for External Antennas 12
A Typical Extricom Wireless Network Topology 13
Switch Cascade 15
Extricom Support for 802.11n 17
Brief Overview of 802.11n 17

Chapter 2 Installing the Extricom WLAN System **20**

Unpacking the Extricom WLAN System 20
Additional Equipment 20
Determining the Location of the Extricom Access Points 21
MS-500/1000 Switch 21
Extricom RP-30n/40En/22n/32n/22En Access Points 24
Connecting the Switch and the Access Points 27
Mounting the Access Points (Optional) 28
Connecting the LS-3000 Switch 29
Range Extenders and Media Converters 31
EXRE-1000 Range Extender 31
EXMC-1000 Media Converter 31

Chapter 3 Configuring the Extricom WLAN System **32**

Accessing the Extricom Switch GUI 32

Using the Extricom Web Configuration Pages....33
Configuring LAN Parameters....36
Configuring WLAN Settings....38
Configuring ESSID Definition....38
Configuring WLAN Radios....53
ESSID Assignment....59
Powering Access Points....61
System Tools Configuration....64
Apply....64
Reboot....65
Maintenance....65
Time & Date....68
Passwords....69
Upgrade....70
Certificate....70
Application....71
License....72
Installing Switch Cascade....74
Advanced Configuration....75
Redundancy....76
Rogue....81
System Logging....82
SNMP....83
Centralized Configuration....84
IDS....87
Portal (Captive Portal)....90
Multicast....92
LBS....93
Expert....93
Others....94
Viewing Events and Reports....95
Overview of the Configuration....102

Chapter 4 Configuring the Extricom LS-3000 System....104

The Extricom LS-3000 Solution....104
The Extricom LS-3000 Switch....104
The Extricom Edge Switch....104
Access Points....104
Media Converter (Optional)....104
Extricom Network Management System (NMS)....104
Redundancy....105
Unpacking the Extricom LS-3000 System....105
Connecting the LS-3000 Switch....105
Accessing the Extricom LS-3000 Switch GUI....106
Using the Extricom Web Configuration Pages....107
Using the Quick Setup Wizard....109

Configuring LAN Parameters....114
Configuring WLAN Settings....116
Configuring ESSID Definition....116
Configuring WLAN Radios....116
Powering EDGE Switches....118
System Tools Configuration....120
Advanced Configuration – LS-3000 Differences....120
Redundancy....120
Multicast....121
Viewing Events and Reports....121
Overview of the Configuration....122

Chapter 5 Troubleshooting....124

Chapter 6 Northbound SNMP Traps....126

Appendix A Internal Access Point Mounting Template....135

About This Guide

This guide provides detailed instructions for installing, configuring, and troubleshooting the Extricom MS-500/1000 and LS-3000 WLAN switches and Extricom RP-30n/22n/32n and 40En/22En UltraThin™ Access Points (APs).

This version of the user guide has been updated to include product changes in the switch version 4.6.05.05.

Audience

This guide is intended for enterprise IT managers and system installers who are familiar with installing and configuring networks.

Conventions

This is a note. A note emphasizes important for the users information.

This is a caution. A caution warns of possible damage to the equipment if a procedure is not followed correctly.

A warning alerts the user of important operating instructions.

Safety Precautions

Follow the instructions in the guide to ensure proper installation and operation of the switch and APs.

The use of wireless devices is subject to the constraints imposed by local laws.

- Operate the switch and APs in an indoor environment.
- Disconnect the switch and APs from power sources before servicing.

- The switch and AP enclosure must not be opened by anyone other than an authorized service representative.
- To comply with FCC RF exposure compliance requirements, maintain a minimal separation distance of at least 20 cm/8 inches between the AP and all persons.
- The power cable included should not be used with any other electrical equipments other than Extricom switches.
- The switch contains an internal battery.
-

!
- ***CAUTION - Always replace the battery with the same type to avoid the risk of explosion.***
- ***Dispose of used battery according to the instructions provided with the new battery.***

Chapter 1

Introduction to the Extricom Wireless LAN System

A Wireless Local Area Network (WLAN) based on the IEEE 802.11 standard enables laptops, PDAs, phones, and other "Wi-Fi" equipped devices to wirelessly connect to the enterprise network.

However, large scale deployments of traditional cell-based WLANs, in which each access point (AP) operates on a different channel than that of adjacent APs, have been hindered by issues such as poor coverage, low capacity, high-latency mobility, and expensive interference analysis or site survey and maintenance costs.

Extricom's WLAN, on the other hand, takes a different and novel solution approach, by avoiding the coverage and capacity trade-offs of traditional cell-based WLAN architecture. In addition, the need for cell planning and interference analysis, a highly expensive aspect of owning a WLAN, is also eliminated. Finally, Extricom's innovative approach does away with most WLAN maintenance tasks. Extricom's WLAN System is specifically designed to provide increased network capacity, seamless mobility, high level of security, and easy installation and configuration.

Overview of the Extricom WLAN System

The Extricom WLAN consists of a wireless switch (M500/1000 connected to a set of UltraThin™ APs (RP-30n, RP-40En, RP-22n, RP-32n and RP-22En). The Extricom WLAN system eliminates the concept of cell-planning and replaces it with the "Channel Blanket" topology. In this topology, each Wi-Fi radio channel is used on every access point to create continuous "blankets" of coverage. By using multi-radio APs, the Extricom system is able to create multiple overlapping Channel Blankets from the same physical set of devices, as illustrated in Figure 1.

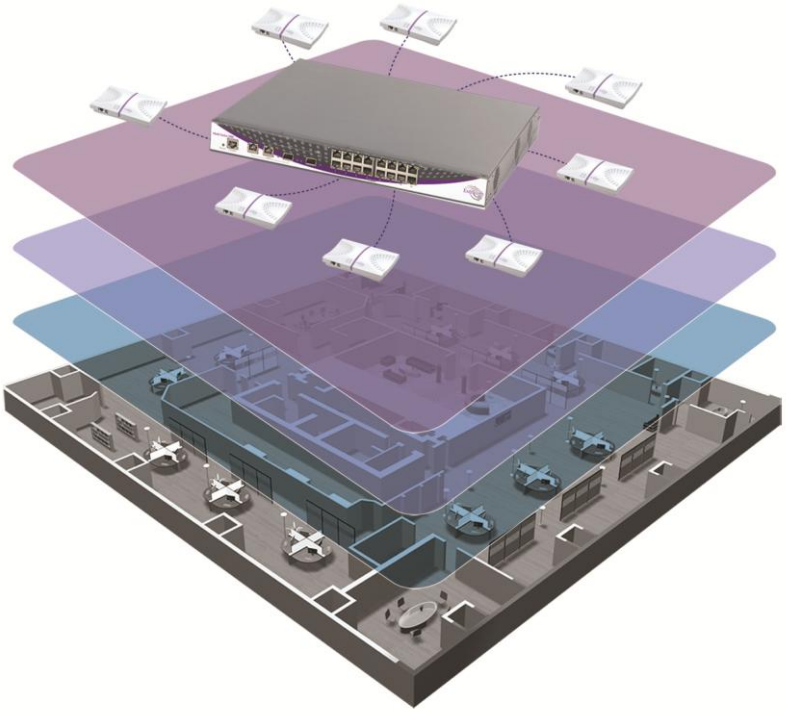


Figure 1: Three Channel Blanket Coverage

The Extricom solution is based on a fully centralized WLAN architecture, in which the switch makes all the decisions for packet delivery on the wireless network. In this configuration, the access points (APs) simply function as radios, with no software, storage capability, or IP addresses. Even the basics of connecting are different: clients associate directly with the switch, not with the APs. The APs act as "RF conduits" to rapidly funnel traffic between the clients and the switch. The Extricom architecture has essentially centralized the 802.11 logic in the switch, while distributing the wireless electronics in the APs.

Centralization of the Wi-Fi environment enables enterprises to deploy 802.11a/b/g/n channels at *every* AP, creating multiple overlapping "Channel Blankets" that leverage each of the radios in the multi-radio UltraThin AP. Each channel's bandwidth is delivered across the blanket's service area (i.e. the combined coverage of all APs connected to the switch), with interference-free operation and consistent capacity throughout.

As the client moves through the coverage blanket, different APs take over the communication with it, depending on which AP is in the best position to serve the client at the time. The switch always uses the optimal uplink and downlink path. While this goes on "behind the scenes," the client never detects an AP-to-AP handoff (i.e. de-association and re-association), thus experiencing seamless mobility.

Within each Channel Blanket, the switch avoids co-channel interference by permitting multiple APs to simultaneously transmit on the same channel only if they won't interfere with each other. This is the essence of the TrueReuse™ functionality.

Extricom supports the 802.11n standard. 802.11n builds upon existing 802.11 standards. 802.11n can be used in both the 5 GHz and 2.4 GHz frequency bands, introduces enhancements to the MAC and the PHY layer, and makes use of multiple-input multiple-output (MIMO) technology. MIMO is a technology that employs multiple transmitter and receiver antennas to support simultaneous data streams. Such technology is capable of increasing data throughput via enhancements such as spatial multiplexing (data streams), 40MHz channel bonding, Block Acknowledgment and frame aggregation, and use of spatial diversity to increase range.

Features and Benefits

Extricom's WLAN system solution offers the following features:

- **Ease of deployment - No cell planning**
  Extricom's architecture requires no cell planning and experiences no constraints due to RF interference or channelization. Consequently, Extricom APs can be deployed wherever needed, in any density or even varying density, to meet the end-client's desired level of service (stipulated in terms of connection rate). The traditional site survey is therefore reduced to simple examination of the space in order to plan the location of the physical equipment.

- **Multi-Layer WLAN**
  Using multiple radio Access Points, a single set of APs enables deployment of multiple high-data-rate Channel Blankets with overlapping coverage, resulting in multiplied aggregate capacity. Separate Channel Blankets also offer the unique ability to guarantee Quality of Service by physically segregating different types of traffic (based on service class, user type, and administrative privileges) onto different channels.

- **Same band operation**
  The Extricom WLAN system enables WLAN channels, in the same band (e.g. Channel 1, 6, and 11 in 2.4 GHz), to be simultaneously used within the same AP, to form overlapping Channel Blankets using the same physical set of APs. It is possible to configure up to four channels of the same band when using RP-40En APs.

- **TrueReuse bandwidth**
  TrueReuse technology multiplies the bandwidth of a standard 802.11 channel by dynamically optimizing the reuse of each frequency. Within a Channel Blanket, up to three APs are permitted to simultaneously transmit on the same channel, when the TrueReuse algorithm determines that they can do this without causing each other co-channel interference.

- **Zero-latency mobility**
  In an Extricom WLAN, wireless device remains on the same channel everywhere within the Channel Blanket. Inter-AP handoffs delays or packet loss do not occur as the client moves across the range of different APs.

- **Wi-Fi Collaboration**
  Extricom's patented Wi-Fi Collaboration technology in which all APs are able to receive on the same channel, provides uplink path diversity for client transmissions, making the system highly resistant to RF instabilities and outside interference.

- **Dense AP deployment**
  In an Extricom WLAN, APs can be deployed in any density convenient to the enterprise, to achieve both blanket coverage and a guaranteed communications rate to all users. In fact, while

cell-based solutions shy away from dense deployments because of their inherent RF obstacles, Extricom's system performance actually increases with AP density.

- **Wire-line quality VoWLAN**
  Extricom's Interference-Free architecture is perfectly suited for VoWLAN providing zero-latency mobility, voice and data separation, reduced power consumption, and high RF resiliency, all together resulting in superior voice performance.

- **IEEE 802.11n**
  Extricom architecture supports 802.11n both in the 2.4 GHz and in the 5GHz bands, using both 20MHz and 40MHz wide channels. The advantages of Extricom's architecture are numerous in the 802.11n setting. Among them is the unique ability to deliver full-bandwidth performance in the 2.4GHz band, to both 802.11n and 802.11b/g devices. By contrast, cell-planning architectures cannot be used with 802.11n 40MHz channel-bonding, since the number of non overlapping channels is insufficient for this.

- **IEEE 802.11i support**
  Extricom's products support WEP-64, WEP-128, WPA-TKIP, WPA2-AES (CCMP) encryption. The authentication modes supported include: RADIUS (802.1x) and WPA Pre-Shared Key (PSK).

- **Power save**
  Full power conservation management is enabled for associated mobile devices over unicast, multicast, and broadcast frames. This is based on various IEEE 802.11 standard power-save specifications such as PS-Poll and U-APSD for 802.11a/b/g devices, and SM & U-PSMP power save for 802.11n devices.

- **Centralized configuration**
  New switches are added to the network via a single Web interface either manually by the user, or automatically using an Extricom protocol.

- **System redundancy**
  Extricom enables full redundancy by connecting two switches in a cascade or hot-standby topology. The switchover parameters are user-configurable.

- **Subnet roaming**
  Subnet roaming enables VLAN and subnet assignments, access control lists, authentications, QoS levels, and other policies to remain with users over the wired-to-wireless transition, regardless of where the user roams in the network. A tunnel is created for a user that roams to a different VLAN while currently communicating with the original VLAN to enable uninterrupted communication.

- **Inter-switch handoff/Fast roaming**
  Extricom enables mobile voice clients to roam seamlessly by supporting fast handoffs between multiple APs and switches in the network. This enables the client to roam back to a previously-authenticated AP with no delay.

- **SNMP**
  The Extricom system supports SNMP V2 based on standard and private MIBs, enabling the user to configure the switch using SNMP Set operations, read switch status using SNMP Get operation and determine the status of the system, including the status of APs and Redundancy, using SNMP Traps. SNMP is provided for customers wishing to use their existing network management system to administer multiple Extricom switches. Alternatively, the EXTRICOM NMSnetwork

management software platform is available as a dedicated centralized Extricom WLAN management system.

- **Multiple RADIUS & RADIUS Redundancy**
  The Extricom system supports multiple RADIUS servers per ESSID, enabling the user to set redundancy between these RADIUS servers. RADIUS is a common authentication protocol utilized under the 802.1x security standard (often used in wireless networks). It improves the WEP encryption key standard, when used in conjunction with other security methods such as EAP-PEAP. In an enterprise environment, several RADIUS servers may be used for backup and also for serving different geographical locations. Up to four different RADIUS servers can be defined for each ESSID. RADIUS redundancy is based on the assumption that the user database is identical in all RADIUS servers and that users are listed in all servers with the same credentials. Switchover from one RADIUS server to another takes place after consecutive failures of the server. The order of priority is 1 to 4.

- **Network Time Protocol (NTP)**
  The Extricom system supports synchronization of the system clock over the network, thereby ensuring accurate local time keeping with reference to radio and atomic clocks located on the Intranet and/or Internet.

- **Fast Handoff (Opportunistic Key Caching)** - WLAN clients roaming between APs of the same channel blanket within a single switch's coverage area experience zero-latency mobility. Clients roaming between different Extricom WLAN switches use the standard 802.11 handoff mechanism, which is further facilitated by the opportunistic key caching mechanism in the 802.11i standard. In addition to this, the Extricom system speeds up 802.11i handoff between Extricom switches by use of Extricom's inter-switch protocol. This permits the client to avoid repetitive 802.1x authentications, thereby enabling faster transition between Access Points connected to different switches with minimal session interruption.

- **Real-time location services –** Based on **AeroScout** technology, Real-Time Location Services (RTLS) technology provides the ability to locate and position mobile wireless network devices (or any user equipment specifically equipped with an AeroScout active RFID tag device), within the Extricom wireless network infrastructure. Extricom products are enhanced to provide support for RTLS by integration with AeroScout active RFID technology. Generally, device location is determined based on several APs picking up a radio transmission attribute from an AeroScout Tag device or any Wi-Fi client, performing measurements and reporting the measurements to an AeroScout Location Engine. AeroScout positioning algorithms use RSSI (Received Signal Strength Indicator) to determine object location. (not available in 3.4).

- **Captive Portal –** The Captive Portal technique compels any HTTP client to view a special web page (usually for authentication purposes) before accessing the rest of the network. Captive Portal turns a Web browser into a secure authentication device. This is done by intercepting an internet access request and redirecting it to an Extricom local logging web page which may require authentication, or simply display an acceptable use policy and require the user to agree.

- **MAC authentication –** MAC authentication technique enables the Extricom switch to authenticate WLAN devices via RADIUS server even if they have no native support for 802.1x. This mechanism is normally used in "dumb" device WLAN topology (such as barcode readers) where WLAN client authentication must be managed via a central RADIUS server.

  - **WMM** - Wi-Fi Alliance WMM is an 802.11 quality of service (QoS) implementation based on **a** subset of the draft 802.11e standard supplement. The WMM specification provides basic

prioritization of data packets based on four categories - voice, video, best effort, and background.

Prioritization is based on the original Carrier Sense Multiple Access/Collision Avoidance Protocol in the 802.11 standard. In 802.11 the Distributed Coordination Function (DCF) mechanism uses a simple *listen-before-talk* algorithm to minimize the chance of packet collisions caused by more than one device accessing the wireless medium at the same time. A client must wait for a randomly selected time period and then "listen" to find whether any other device is communicating before starting to transmit. The random back-off period gives all devices a fair opportunity to transmit.

WMM (based on 802.11e standard) enhances the DCF by defining an Enhanced Distributed Channel Access (EDCA). EDCA specifies different fixed and random wait times for the four prioritization categories to provide more favorable network access for applications that are less tolerant of packet delays. Devices that have less time to wait have a better chance of being able to transmit than those that have a longer wait. In order of highest priority, the access prioritization categories are *voice, video, best effort* and *background*.

By default, these four WMM prioritization categories are statically mapped to Ethernet 802.1p prioritization tags to allow consistent QoS across wireless and wired network segments. Flow arriving from the wired network tagged with 802.1p priority is mapped to the appropriate Access category, while WMM flow arrived from the wireless medium is encapsulated and tagged with the appropriate 802.1p priority.

The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space Number (AIFSN) followed by a random period called the Contention Window (CW), both specified in multiples of the slot time. The CW maintains the DCF random back-off component to help avoid collisions of packets from the same access category. The CW range doubles each time there is a collision (starts CWmin up to CWmax) and is reset to its minimum value after a successful transmission.

EDCA uses a mechanism called a Transmit Opportunity (TXOP) – a bounded time interval during which a station can send as many frames as possible, but the transmission time must not extend beyond the maximum duration of the TXOP. Each priority level is assigned a TXOP, and this mechanism prevents low speed stations from spending too much time using the media when other clients (including those with traffic in higher priority queues) are waiting.

Another mechanism introduced by WMM is per access category Acknowledgment policy (Normal or No ACK); Normal means that acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. However one may choose to cancel the acknowledgement by selecting "No ACK" for each access category. This can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.

- **WMM** – The WMM defined by Wi-Fi alliance is an 802.11 quality of service (QoS) implementation based on a subset of the draft 802.11e standard supplement. The WMM provides over-the-air service quality by defining Access Categories and associating each with different WLAN parameters, such as contention windows. Flow arriving from the wired network is statically mapped to the Access Categories based on its 802.1p or TOS/DSPC values.

- **Extricom NMS** – The Extricom Network Management System (NMS) is a comprehensive tool that enables System Administrators to manage any size of Extricom WLAN from a single interface. Employing the FCAPS (Fault/Configuration/Accounting/Performance/Security) network management model and a Client/Server architecture, the Extricom NMS seamlessly

connects with Extricom's complete line of enterprise switches and access points, providing easy, standards-based systems administration, configuration, and monitoring.

- The EXTRICOM NMS supports medium-to-large-scale enterprises that have deployed up to 2,000 Extricom WLAN switches. It runs on standard enterprise server platforms and uses an optional MySQL 5.0 database to maximize affordability and flexibility.
- **Blanket balancing**
  The switches automatically perform load balancing, distributing the traffic evenly over the different channels.

Overview of the Multi Series (MS) Switch Platform

The Extricom WLAN switches are connected to Extricom APs to form an Extricom WLAN. The Extricom Multi Series (MS) is a high-performance switch hardware platform, and is software-configurable to support a range of wireless and networking functions in an Extricom WLAN System.

Figure 2: Extricom MS-1000

The MS-1000 is equipped with two RJ45/SFP GBE Combo port uplinks, and 16 GBE PoE (Power over Ethernet) edge-side ports. The MS-1000 is capable of performing different wireless and networking functions, depending on the firmware installed on it.

Figure 3: Extricom MS-500

The MS-500 is equipped with two RJ45/SFP GBE Combo port uplinks, and 8 GBE PoE edge-side ports. The MS-500 is capable of performing different wireless and networking functions, depending on the firmware installed on it.

Configuring a switch and its associated set of APs is as simple as configuring a single traditional AP, greatly reducing the effort required to deploy and maintain the WLAN. Configuration is done via a dedicated, secured Web interface that comes standard with every switch, or via the optional EXTRICOM Network Management System (NMS).

SFP modules are not shipped with the MS-500/1000. To use the SFP ports, you must use Class 1 laser certified SFP modules according to IEC/EN 60825-1 and /or CDRH.

Overview of the Extricom Access Points

Access Points with Internal Integrated Antennas

The 3-radio Extricom RP-30n is an 802.11a/b/g/n access point with internal antennas, for maximum throughput and easy deployment of 802.11n with or without legacy Wi-Fi. The RP-30n is equipped with two a/b/g/n radios and one a/b/g radio, each of which can be operated on the 2.4 GHz or 5 GHz band. Each ‘n' radio has a 3x3 MIMO antenna configuration for an air rate of up to 300 mbps.

The 2-radio Extricom RP-22n and the 3-radio Extricom RP-32n are 802.11n access points with internal antennas for maximum throughput and easy deployment of 802.11n with or without legacy Wi-Fi. The RP-22n is equipped with two and the RP-32 - with three dual-stream radios, each of which can be operated on the 2.4 GHz or 5 GHz band. Each radio has a 2x2 MIMO antenna configuration for an air rate of up to 300 mbps.

The APs do not require configuration, enabling plug-and-play installation. If stolen, the APs do not pose a security risk, since all encryption is performed in the switch.

With all intelligence residing in the WLAN switch, APs may be placed as close together as necessary to provide high-quality, high-speed connectivity from all locations within the enterprise.

Extricom APs are connected to the Extricom WLAN Switch via standard Cat5e/6 cables. The APs are powered by the standard 802.3af Power over Ethernet (PoE), and only a single Cat5e/6 cable connection is required to support all radios in an Extricom AP.

An EXRE- 1000 range extender can be used between the AP and the switch, for extended reach.

Figure 4: Extricom RP-22n/32n AP

Figure 5: Extricom RP-30n AP

Access Points with Connectors for External Antennas

Some applications may require an access point capable of connecting to external antenna(s). The Extricom RP-22En and RP-40En accommodate this requirement. The RP-40En contains two 802.11a/b/g/n radios and two 802.11a/b/g radios. The RP-40En has ten external antenna connectors. The RP-22En contains two dual stream 802.11a/b/g/n radios and four external antenna connectors.

An external antenna may be desired to make the AP less visible by mounting it in the plenum. The situations may arise, where to ensure connectivity and service levels within a complex coverage environment, directional antennas may be needed, rather than the omni-directional antennas that are standard inside Extricom integrated antenna APs. In such cases, the antennas may also be located at some distance from the AP in order to cover a specific area.

Figure 6: Extricom RP-22En/40En AP

The RP-22En and RP-40En APs are connected to the Extricom WLAN Switch via standard Cat5e/6 cables, in exactly the same manner as integrated antenna AP models. The APs are powered by the standard 802.3af Power over Ethernet (PoE), but can be powered by an external power supply if desired.

An antenna with an RP-SMA plug (male) connector can be connected to the RP-22En and RP-40En. For purposes of product homologation testing, Extricom used a "Rubber Duck"-type antenna, specifically the Netgate 2.4-2.5 / 5.1-5.9 GHz Dual Band Rubber Duck RP-SMA (part number: ANT-2458-5RD-RSP). More specifications on this antenna can be found at http://www.netgate.com/product_info.php?products_id=386.

! With RP-22En/40En - Use only xPVC or similar jacket cable which is NEC Article 725 and 444 Compliant and plenum rated per NFPA 262 (UL 910) standard

A Typical Extricom Wireless Network Topology

An Extricom WLAN switch is connected to the wired LAN, and the APs distributed throughout the enterprise. Figure 7 shows a typical Extricom enterprise topology, consisting of an Extricom switch and eight APs.

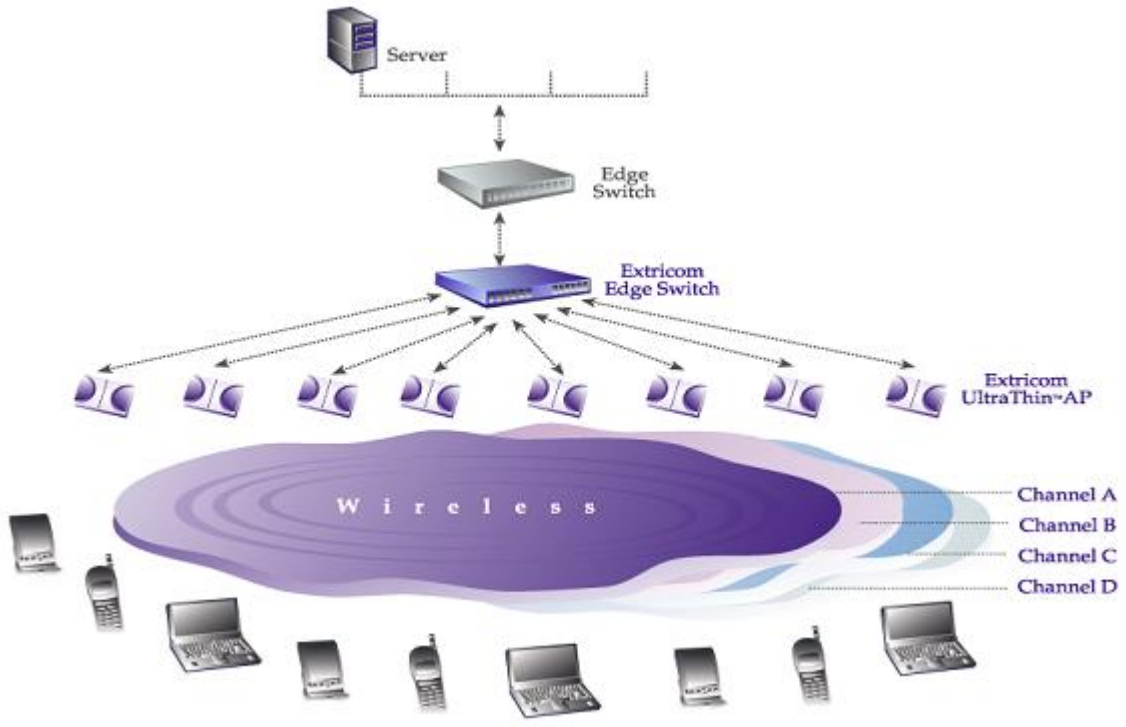


Figure 7: Typical Extricom Typology

Extricom uses standard WLAN protocols (IEEE 802.11). As a result, any 802.11a/b/g/n standard wireless device can work seamlessly with the Extricom system.

- **<u>Mixing different types of Extricom APs on the same switch is not permitted</u>, except in the following cases:**
  - **RP-30n and RP-40En.**
  - **RP-22n, RP-32n and RP-22En**

IMPORTANT NOTE: While these AP configurations are possible, it should be noted that this may result in a heterogeneous wireless coverage between the different channel blankets throughout the deployment area.

- **Extricom APs must be directly connected to the switch to function.**
- **An Extricom range extender or media converter may be used between the AP and the switch, when extra range is required.**

Switch Cascade

Switch Cascade is an Extricom topology in which two MS-1000 switches are interconnected together to create one larger logical switch with optional enhanced redundancy capabilities. One MS-1000 switch serves as the primary, and the other MS-1000 switch serves as the secondary. A diagram of the Cascade topology is shown below, in its standard configuration:

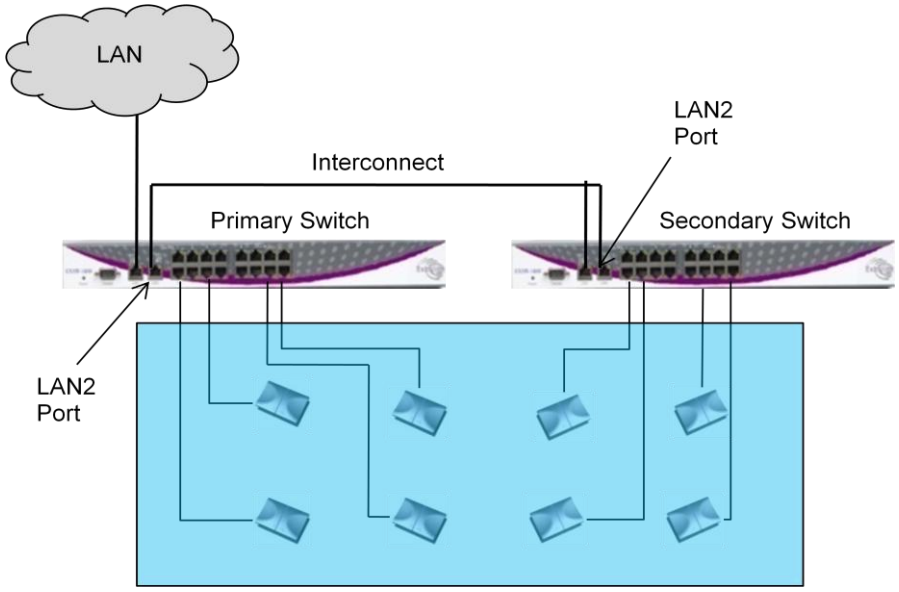


Figure 8: Switch Cascade Topology

The interconnect hardware is connected to the LAN2 port of each switch. See page 26 for more details about the interconnect hardware and maximum distance between cascaded switches.

The APs of both switches together form a seamless channel blanket. Up to 4 seamless channel blankets can be deployed. Up to 32 APs can be deployed in a cascade topology.

In the Figure 9 above, a basic Switch Cascade configuration is depicted.

In a switch cascade, the secondary switch routes all of the traffic from its APs to the primary switch over the interconnect cable. The primary switch performs the full set of Extricom edge switch functions on the secondary switch's traffic, as well as on the traffic from its own APs. It determines to which AP to transmit each incoming packet, while the secondary switch forwards the traffic it receives to the correct AP.

Heartbeat checks are performed over the LAN links. A failover takes place if there is a critical failure of one of the switches, one of the LAN links, or the interconnect hardware.

Resiliency in Switch Cascade

The optional Resiliency licensed feature provides enhanced redundancy capabilities through several layers – Switches and APs and combined. See following examples below:

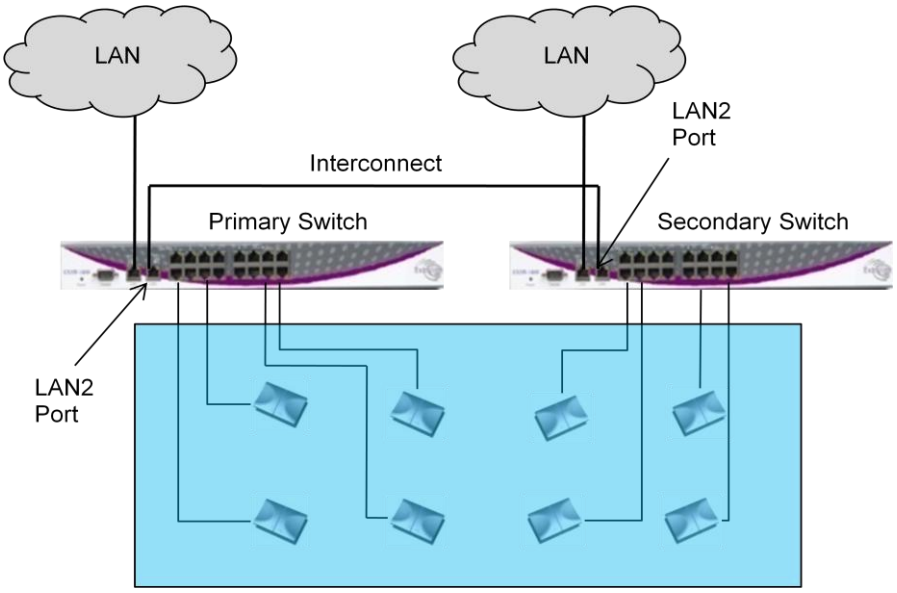


Figure 9: Uplink Port Redundancy in Switch Cascade Topology

In the Figure 10 above, the switch configuration provides uplink port redundancy - if the Primary switch uplink connectivity is lost for some reason, the secondary switch takes over the primary switch and replaces its functionality with no loss of wireless service. In this configuration there's no redundancy in APs deployment, and each AP covers a specific area uniquely.

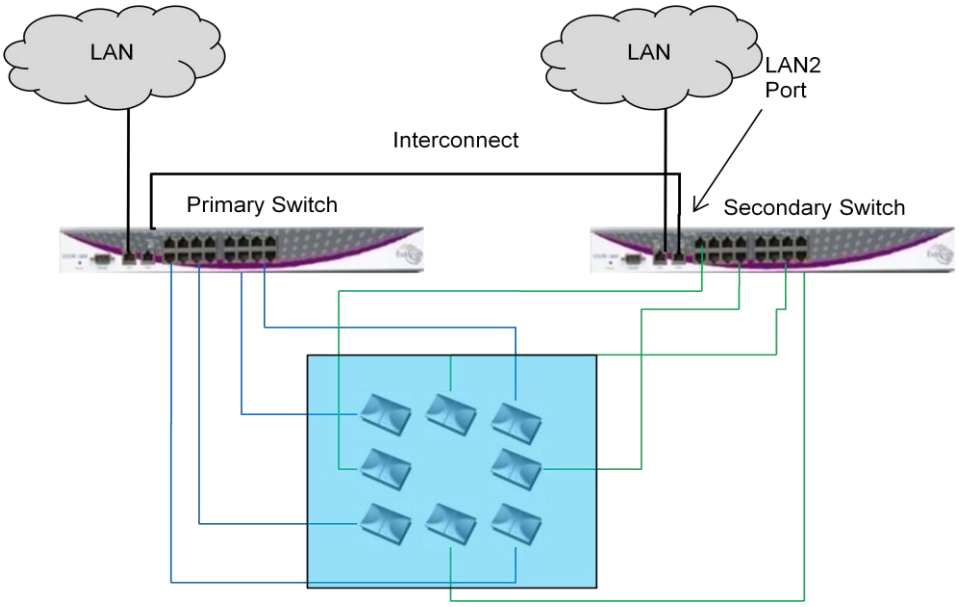


Figure 10: AP Redundancy in Switch Cascade Topology

In Figure 10 above, an AP redundancy configuration is shown, where it's possible to deploy APs interleaved, depending on the degree of service robustness required in the event of a failure. In an

AP interleaved deployment, most APs are configured as in Figure 10, but one or more APs from the Primary Switch are placed in the coverage area of the Secondary Switch, and vice versa. Such cross-connect provides necessary redundancy and prevents failure in wireless coverage when one of the switches, Primary or Secondary, fails.

Extricom Support for 802.11n

802.11n is a breakthrough technology that enables Wi-Fi networks to do more, faster, over a larger area. 802.11n Wi-Fi provides optimized connectivity for enterprise computer networking, delivering the range, bandwidth, and performance that multimedia applications and products demand.

For 802.11n deployment, Extricom offers the RP-30n, and RP-40En APs. The RP-30n contains two 802.11a/b/g/n radios and one 802.11a/b/g radio, and the RP-40En contains two 802.11a/b/g/n radios and two 802.11a/b/g radios.

Brief Overview of 802.11n

The following section describes at a high level the main features and terms of 802.11n. It also outlines which features of the standard are supported by Extricom products at this time. This section is provided to give customers using Extricom's 802.11n products an overview of 802.11n technology, and to help them understand what parameters need to be to configured on the Extricom switch in order to support 802.11n.

802.11n is a member of the 802.11 family of standards; it can function in both the 2.4 GHz and 5GHz bands using OFDM transmission (as with 802.11a and 802.11g). The emphasis in 802.11n design was mainly on increasing bandwidth, range and performance of the 802.11 protocol itself. This was largely achieved by using multiple transmitters/receivers (MIMO) and enhancements to the OFDM PHY and 802.11 MAC layers.

MIMO

Definition: 802.11a/b/g devices used SISO architecture (single input, single output) for transmitter and receiver paths. 802.11n uses MIMO **(**Multiple inputs / multiple outputs) architecture. That is, multiple transmitter and multiple receiver antennas **(NxM)** are used to support multiple, simultaneous data streams**.**

Extricom 802.11n: Extricom Access Points support both 2x2 and 3x3 MIMO configuration.

Data Streams

Definition: Spatial multiplexing divides data into multiple streams and sends it simultaneously over multiple paths using the multiple transmitters (antennas) over the channel. These streams are recombined by the multiple receivers to get the original data. Different Extricom Access Point models support dual and triple data streams over the 2x2 and 3x3 transmitter/receivers radio configuration.

Channel Bonding

Definition: All earlier versions of 802.11 have used 20 MHz wide channels, defined in the 2.4 GHz and 5 GHz bands. 802.11n- Draft 2.0 specifies operation in the same 20 MHz channels used by 802.11b/g in the 2.4 GHz and 802.11a in the 5 GHz bands, but adds a mode where a full 40-MHz wide channel can be used. This offers approximately twice the throughput of a 20-MHz channel.

Extricom 802.11n: Extricom products support 20 and 40MHz channels *both* in 2.4GHz and 5GHz.

Guard Interval

Definition: In OFDM, inter-symbol interference occurs when the delay between different RF paths to the receiver exceeds the guard interval, causing a reflection of the previous symbol to interfere with the strong signal from the current symbol: a form of self-interference. 802.11n allows a shorter guard interval to increase PHY performance.

Extricom 802.11n: Extricom supports configurable guard interval (400 or 800 ns). However, short guard interval is only supported with 40MHz channel.

Frame Aggregation

Definition: With MAC-layer aggregation, a station with a number of frames to send can combine them into an aggregate frame (MAC MPDU). The resulting frame contains fewer headers in overhead than would be the case without aggregating, and because fewer, larger frames are sent, the contention time on the wireless medium is reduced.

Extricom 802.11n: Extricom supports frame aggregation.

Block Acknowledgment

Definition: Block Acknowledgment works in conjunction with frame aggregation, allowing the transmitter to request a block ACK for a multiple frame improving overall performance.

Extricom 802.11n: Extricom supports block acknowledgment.

Operating Modes

Definition: 802.11n defines three modes of operation for 802.11n devices:

1. Legacy mode – In this mode, the 802.11n radio works in legacy 802.11a/b/g mode only.
2. Mixed mode – In this mode the 802.11n radio can work with both 802.11n & 802.11a/b/g clients
3. Greenfield mode – In this mode the 802.11n radio works only with 802.11n clients.

Extricom 802.11n: Extricom products support both Legacy and Mixed modes. Currently there is no support for Greenfield mode. With this release, however, Extricom is introducing a unique feature, the "**HT Only**" blanket in which a specific Channel Blanket can be configured so that only 802.11n clients (working in mixed mode) can associate with it. This enables support of co-existence of 'n' and 'b/g' clients, from the same set of APs, but separated on different channels, so there is no mixed-mode throughput degradation.

Coexistence

Definition: 802.11n is designed to operate with backward compatibility for 802.11b/g/a devices—the method of operation known as mixed mode that was previously described. 802.11b/g/a, on the other hand, does not have forward compatibility with 802.11n. Therefore 802.11n must protect 802.11b/g/a stations from 802.11n transmissions that may be interpreted as interference.

Extricom 802.11n: Extricom supports PHY layer protection (L_SIG protection) for OFDM transmissions (802.11a/g clients). MAC layer protection is supported (Dual CTS protection) for non-OFDM (802.11b) clients.

MCS

Definition: The complexity of 802.11n rate adaptation has given birth to the concept of Modulation Coding Scheme (MCS). MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream.

Extricom 802.11n: Extricom supports two data streams; therefore MCS 0 to 15 can be configured.

SM Power Save

Definition: The basic 802.11n power save mode is based on the earlier 802.11 power save function. Power save in 802.11n is enhanced for MIMO operation with SM power save mode. Since MIMO requires maintaining several powered-up receiver chains, standby power draw for MIMO devices is likely to be considerably higher than for earlier 802.11 equipment. A new provision in 802.11n allows a MIMO client to power-down all but one RF chain when in power save mode. When a client is in the 'dynamic' SM power save state, the AP sends a wake-up frame, usually an RTS/CTS exchange, to give it time to activate the other antennas and RF chains. In static mode, the client decides when to activate its full RF chains, regardless of traffic status.

Extricom 802.11n: Extricom supports SM power save mode static mode.

Chapter 2

Installing the Extricom WLAN System

This chapter provides instructions for unpacking and installing the Extricom WLAN system.

Unpacking the Extricom WLAN System

The Extricom WLAN system is shipped with the following:

- One Extricom switch.
- CD which contains The Extricom WLAN System User Guide, Release Notes and EULA.
- APs (the number of APs is based on customer order and provided in separate boxes) are shipped as part of the overall order.
- One power cable.
- Mounting brackets with screws.

The Extricom WLAN LS 3000 system is shipped with the following:

- One Extricom LS-3000 switch.
- MS 1000 (EDGE) switches (the number of EDGE switches is based on the customer order and provided in separate boxes) are shipped as part of the overall order.
- CD which contains license serial number
- APs (the number of APs is based on customer order and provided in separate boxes) are shipped as part of the overall order.
- One power cable.
- Mounting brackets with screws.

Additional Equipment

The following additional equipment is required for installing the Extricom WLAN system:

- One CAT-5e/6 cable for each AP.
- One CAT-5e/6 cable(s) for connecting the WLAN switch uplink to the LAN switch.
- A range Extender (EXRE-1000) is required for any AP that will be located between 100 and 200 meters from the WLAN switch.

- For cabling distances over 200 m, EXMC-1000 media converters must be used.
- Two stainless steel pan head 8x1-1/4" self-tapping Phillips screws for wall or ceiling mounting each AP (optional).

Determining the Location of the Extricom Access Points

Before installing the switch and the APs, create a plan for the placement of the APs. Before permanently mounting the APs, Extricom recommends testing the network (using a laptop client) to identify potential coverage holes. If such a problem exists, relocate an AP or add more APs to eliminate the holes in the coverage. To find the best location for the required coverage, the Extricom Deployment Tool may be used.

The APs should be placed in a stable, secure location, such as on top of a closet or a bookshelf, or mounted on a wall.

The switch should be placed near the distribution point of the LAN line. This is usually in the communications closet of your enterprise.

MS-500/1000 Switch

The Extricom MS-500 Appliance Platform has 13 connectors (refer to Figure 11)

The Extricom MS-1000 Appliance Platform has 21 connectors (refer to Figure 12).

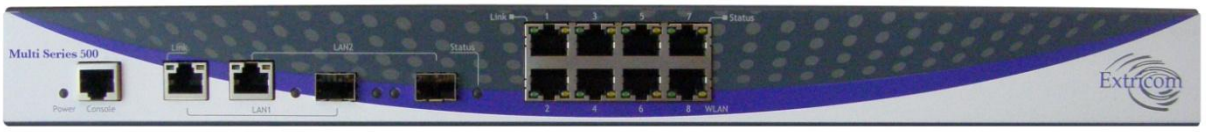


Figure 11: Extricom MS-500 Switch

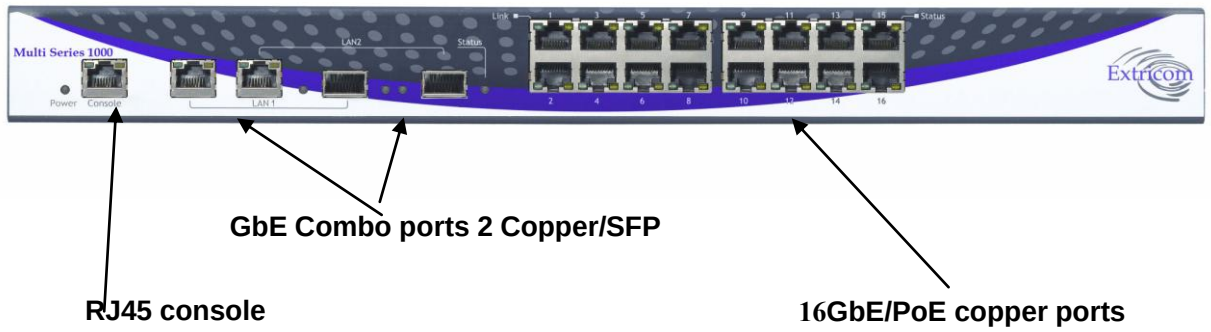


Figure 12: Extricom MS-1000

Figure 13: Extricom LS-3000

Table 1 below describes the front panel and connectors of ExtricomMS-500/1000 switches.

Connectors	Description
Console	Serial connector – only to be used for troubleshooting, support, or maintenance by, or as instructed by, Extricom personnel. Can be accessed using a Null modem cable.
LAN1,LAN2	2 GbE RJ-45, 2 GbE SFP combo ports – used to connect the switch to the wired LAN. Use only GbE or SPF. Only LAN1 is used for connection to the wired LAN. LAN2 is used for Switch Cascade interconnect only.
WLAN (AP) Ports	RJ-45 connectors – used to connect Extricom APs to the switch. These ports provide 802.3AF PoE compatible power. Maximum current: 270 mA, 48 volts. ***Do not connect any device other than Extricom APs to the WLAN ports.***

Table 1: Extricom Switch Connectors

Table 2 below describes the front panel LEDs of Extricom MS-500/1000 Appliance Platforms.

LED	Color	Description
Power	None	• No power
	Green	• *Blinking* - switch is loading • *Solid On* - switch is ready/operational
	Red	• *On* - Error after loading
	Green-Orange	• *Blinking* - RF localization error
LAN, LAN1, LAN2 Ports		
Act/Link	Green	• *Solid On* - connection • *Blinking* - activity over connection • *Off* - no connection
	Orange	• Not in use. Only a 1000 Mbps LAN connection is supported.
Status (SFP links)	Green	• *On* - 1000 Mbps full duplex SFP connection • *Off* - no SFP connection
WLAN (AP) Ports		
Link	Green	• *On* - connection • *Blinking* - activity over connection • *Off* - no connection
Status	Orange	• *On* - 1000 Mbps full duplex connection • *Off* -100 Mbps full duplex or no connection

Table 2: Extricom Switch LEDs

Extricom RP-30n/40En/22n/32n/22En Access Points

All Extricom APs have two connectors on the front panel of the device - the WLAN connector and the Power connector. Two models - the RP-22En and RP-40En - have external antenna connectors, four and ten respectively. In addition, only two models - the RP-30n and the RP-40En have LEDs on the top surface of the device (See Figure 14 below). The LEDs are: Link, Radio1, Radio2, and Radio3.

Figure 14: Extricom RP- With LEDs 30n

Figure 15: Extricom RP-40En - With LEDs

The other four AP models, RP-22n, RP-32n (see Figure 16 below), and RP-22En (see Figure 16) each have only one LED located near the LAN port on the front face of the device. This LED indicates the status of the AP.

Figure 16: Extricom RP-22n/32n - Without LEDs

Figure 17: Extricom RP-22En - Without LEDs

The three tables below describe the Extricom Access Point connectors and LEDs.

Connectors	Description
Power	External power is not required for most applications. Power is supplied via the Ethernet cable (PoE). In case of an external power requirement (e.g. when media converters are used and POE is blocked), use a UL Listed LPS (Limited Power Source) or NEC Class II power adapter. Rating – Input: 90-240VAC, 0.8A max. Output: 48VDC, 0.56A max. The DC output plug of the power supply must be a standard round DC plug with 5.5mm outer ring diameter and 2.5mm inner ring diameter. Plug polarity: Outer (-), Inner (+). ***Due to regulatory requirements in Europe (CE) and the pending certification process for the power supply connector, an external power supply should not be used with EXRP20/40/20E/40E.***
WLAN	RJ-45 connector – used to connect the Extricom AP to the Extricom switch. Power is provided by the Extricom switch to the AP when directly connected to it.

Table 3: Extricom AP Connectors

LEDs	Color	Description
Radio 1	Green	1st Radio is active
	Red	1st Radio is enabled with no assigned ESSID, or malfunctioning
	Off	1st Radio is off
Radio 2	Green	2nd Radio is active
	Red	2nd Radio is enabled with no assigned ESSID, or malfunctioning
	Off	3rd Radio is off
Radio 3	Green	3rd Radio is active
	Red	3rd Radio is enabled with no assigned ESSID, or malfunctioning
	Off	3rd Radio is off
Radio 4	Green	4th Radio is active
	Red	4th Radio is enabled with no assigned ESSID, or malfunctioning
	Off	4th Radio is off

Table4: Extricom RP-40En AP LEDs

LEDs	Color	Description
Radio 1	Green	1st Radio is active
	Red	1st Radio is malfunctioning
	Off	1st Radio is off
Radio 2	Green	2nd Radio is active
	Red	2nd Radio is malfunctioning
	Off	2nd Radio is off
Radio 3	Green	2nd Radio is active
	Red	2nd Radio is malfunctioning
	Off	2nd Radio is off
Link	Green (flashing)	Connection to Extricom switch is active
	Off	Not active

Table 5: Extricom RP-30n LEDs

Connecting the Switch and the Access Points

The Extricom switch is connected to the wired LAN and to the APs that are located throughout the enterprise.

To connect a switch and access points:

1. Using a CAT-5e/6 100/1000Mbps cable, connect the RJ-45 LAN1 connector located on the front panel of the switch (refer to Figure 12) to the LAN switch.
2. Using a CAT-5e/6 cable, connect each AP to one of the switch's RJ-45 WLAN connectors.

> If an AP must be located over 100 meters from the switch, an Extricom Range Extender must be used, which allows up to an additional 100m, for a total switch to AP distance of up to 200m.
>
> Switch to AP distances of up to 700m can be supported on GbE connections by using Extricom EXMC-1000 media converters.

3. Connect the power cable to the power connector located on the rear panel of the switch, and plug the other end of the power cable into a power source.
4. Verify that the Power LEDs on both the switch and connected APs are green.

> Additional APs can be connected /disconnected while the switch is active.

> If using fiber media converters (ATI/100Mbps, CTC/1000Mbps) to extend switch-to-AP distance:
>
> - Each converter requires external power
> - Once all cables are connected (Switch – copper – converter – fiber – converter – copper – AP) perform a port power down/up in the web GUI of the switch to renew switch awareness of the AP connection.
> - Fiber mode is Multi for 100Mbps
> - Fiber mode can be Multi or Single for 1000Mbps per the SFP module selected. Note both ends of the fiber termination must be in the same (SFP) mode.

To connect a switch cascade:

1. Connect the primary and secondary switch to the LAN and to its APs, as directed in the section above.
2. Verify that both switches are running the same firmware release, and that this is the newest release that supports Switch Cascade.
3. Refer to the chart on the following page for important switch interconnect guidelines.
4. Connect the switch interconnect cable to the LAN2 port of the primary switch and to the LAN2 port of the secondary switch. ().

The maximum length of the primary to secondary switch interconnect is computed according to the following tables: (all distances are in meters)

Using CAT-5e/6 100/1000Mbps Cable:

Distance Between Secondary Switch and Its Farthest AP	Max. Switch Interconnect Distance (Copper Interconnect Cable)
150 (with EXRE)	50

Note: Beyond 100 m, copper-based cables require a range extender (EXRE).

Using Fiber media Cable:

Distance Between Secondary Switch and Its Farthest AP (*)	Max. Switch Interconnect Distance (Fiber Interconnect Cable)
450 (with EXMC)	50
50 (with EXMC)	450

(*) The total length of the copper-based cable to/from EXMC must be less than 2m.

Using mixed media types:

Distance Between Secondary Switch and Its Farthest AP (Copper cable)	Max. Switch Interconnect Distance (Fiber Interconnect Cable)
100	400
200 (with EXRE)	300

Distance Between Secondary Switch and Its Farthest AP (Fiber cable) *	Max. Switch Interconnect Distance (Copper Interconnect Cable)
450 (with EXMC)	50

(*)The total length of the copper-based cable to/from EXMC must be less than 2m.

Note: EXMC and EXRE are not to be used with uplink ports, like in the case of Interconnect.

Mounting the Access Points (Optional)

Extricom RP-40En and RP-22En APs can be mounted on a wall or the ceiling. For this purpose, a separate mounting bracket is provided for ease of installation. The bracket has two holes for mounting to the wall, and one hole for a screw that mounts the AP to the bracket.

Extricom RP-22n/32n/30n APs can be mounted on a wall or the ceiling without additional mounting brackets. To mount the APs, you will need two stainless steel pan head 8x1-1/4" self-tapping Phillips screws (not supplied).

To mount the RP-22n/32n/30n Access Points:

1. Place the installation template (refer to Internal Access Point Mounting Template in this Guide) on the wall where you want to mount the AP.
2. Mark the "Point for Drilling" locations on the wall.
3. Screw the two stainless steel pan head 8x1-1/4" self-tapping Phillips screws into the wall leaving enough of the screws protruding to enable you to hook the AP over the screws.
4. Align the holes on the back of the AP with the screws and slip the AP into place.

Connecting the LS-3000 Switch

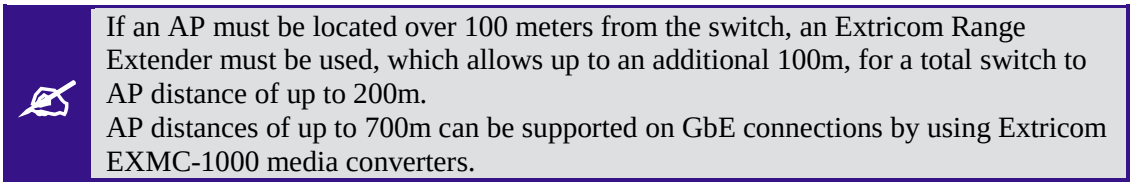
The LS-3000 Switch is designed to greatly increase the coverage area of the Extricom solution. The Large Scale solution is a/b/g/n Wi-Fi-compliant.

The Extricom Large Scale (LS) switch is typically connected to the wired LAN and to between 4 and eight EDGE switch devices. Each EDGE switch connects up to 16 APs that are located throughout the enterprise.

The Extricom Large Scale Switch (LS-3000) attaches to the network via the IEEE802.3ad link aggregation ports. Network configuration details such as security profile, SSIDs, assigned channels to blankets, VLAN assignments, are maintained in the LS-3000 switch, not by the EDGE switches.

To connect an LS-3000 switch to the EDGE switches and access points:

1. Using a CAT-5e/6 100/1000Mbps cable, connect the RJ-45 LAN1 connector located on the front panel of the switch to the LAN switch.
2. Using a CAT 5e/6 100/1000Mbps cable, connect the RJ-45 LAN1 connector located on the front panel of each EDGE switch to one of the LS3000 switch's RJ-45 WLAN connectors.
3. Using a CAT-5e/6 cable, connect each AP (refer to Figure 12) to one of the EDGE switch's RJ-45 WLAN connectors.


If an AP must be located over 100 meters from the switch, an Extricom Range Extender must be used, which allows up to an additional 100m, for a total switch to AP distance of up to 200m.
AP distances of up to 700m can be supported on GbE connections by using Extricom EXMC-1000 media converters.

4. Connect the power cable to the power connector located on the rear panel of the LS-3000 switch, and plug the other end of the power cable into a power source.
5. Connect the power cables to the power connectors located on the rear panel of the EDGE switches, and plug the other end of the power cables into a power source.
6. Verify that the Power LEDs on all the switches and connected APs are green.

Additional APs can be connected /disconnected while the switch is active.

If using fiber media converters (ATI/100Mbps, CTC/1000Mbps) to extend switch-to-AP distance:

- Each converter requires external power.
- Once all cables are connected (Switch – copper – converter – fiber – converter – copper – AP) perform a port power down/up in the web GUI of the switch to renew switch awareness of the AP connection.
- Fiber mode is Multi for 100Mbps.
- Fiber mode can be Multi or Single for 1000Mbps per the SFP module selected. Note both ends of the fiber termination must be in the same (SFP) mode.

The maximum length of the primary to secondary switch interconnect is computed according to the following tables: (all distances are in meters).

Using CAT-5e/6 100/1000Mbps Cable:

Distance Between Secondary Switch and Its Farthest AP	Max. Switch Interconnect Distance (Copper Interconnect Cable)
150 (with EXRE)	50

Note: Beyond 100 m, copper-based cables require a range extender (EXRE).

Using Fiber media Cable:

Distance Between Secondary Switch and Its Farthest AP (*)	Max. Switch Interconnect Distance (Fiber Interconnect Cable)
450 (with EXMC)	50
50 (with EXMC)	450

(*) The total length of the copper-based cableto/from EXMC must be less than 2m.

Using mixed media types:

Distance Between Secondary Switch and Its Farthest AP (Copper cable)	Max. Switch Interconnect Distance (Fiber Interconnect Cable)
100	400
200 (with EXRE)	300

Distance Between Secondary Switch and Its Farthest AP (Fiber cable) *	Max. Switch Interconnect Distance (Copper Interconnect Cable)
450 (with EXMC)	50

(*)The total length of the copper-based cable to/from EXMC must be less than 2m.

Note: EXMC and EXRE are not to be used with uplink ports, like in the case of Interconnect.

Range Extenders and Media Converters

EXRE-1000 Range Extender

The EXRE-1000 Power Over Ethernet Gigabit (PoE) Range Extender doubles the standard range of PoE, from the baseline 100 meters to a full 200 meters, all while enabling full gigabit speed. It can be used both as a standalone product, to extend the reach of PoE installations, and as a complement to the Extricom's WLAN System.

When used in WLAN implementations, the EXRE-1000 enables any Extricom UltraThin™ Access Point to be connected using standard Cat5e/6 cable up to 200 meters from the Extricom WLAN Switch. The Range Extender sits in-line on the Ethernet cable and does not require an external power feed. The Range Extender receives its power from the original PoE injector in the switch or from a PoE injector/power supply, while it simultaneously injects PoE to the extended cable segment.

EXMC-1000 Media Converter

The EXMC-1000 Media Converter allows users to extend the size of their WLAN with the use of fiber cabling. The EXMC-1000 functions as a GbE range extender, providing fiber connectivity to Extricom access points and Extricom WLAN switches at distances of up to 700 meters, assuming that the switches and the APs are GbE-enabled. The EXMC-1000 can be installed in any implementation and is connected to the WLAN switch, the EDGE switch or AP with Cat-5e/6 cable through a standard RJ45 port.

The EXMC-1000 provides an extended level of deployment flexibility for large-scale Channel Blanket deployments, as it does not need the power infrastructure normally required for fiber deployments. The switch-side media converter is powered via PoE from the WLAN switch or optional external power supply; the AP-side media converter is powered via external power supply and provides PoE to the AP. Effectively, a 700-meter fiber run to an AP will require only a single power supply.

Chapter 3

Configuring the Extricom WLAN System

Accessing the Extricom Switch GUI

After connecting the switch and APs, configure the Extricom WLAN system through Extricom's web configuration GUI using a terminal or PC connected to the same LAN as the switch.

To access the Extricom web-based configuration tool:

1. In your Web browser, enter the following: **`https://<IP address of the switch>`** where **`<IP address of the switch>`** is the IP address of the switch provided with your purchase. Note that **https** must be used, *not* http, in order to initiate a secure browsing session (SSL) with the switch.

Prior to opening the configuration tool, make sure your console PC is configured with an IP address in the same subnet as the switch.
If you did not receive a switch IP address with the switch, the factory default value for the switch IP address is 192.168.1.254.

If you are using the default IP settings, do not place a router between the user PC and the switch.

2. On the first login you will receive a notice in your browser that there is a problem with the website's security certificate. Click on "**Continue to this website (not recommended)**".
3. The *Login* page appears, as shown below in Figure 18:

Figure 18: Login Page

4. Enter the user name and password of the system integrator and click **OK**. The *Summary* page appears.

If you did not receive a user name and password with your switch, use the following factory default user name and password:

user name: *admin*
password: *Switch1*

The user name and password are case-sensitive.

If you use Internet Explorer 8 web browser to configure the switch, you will receive a notice in a pop-up window stating that there is a problem with the website's security certificate.

1. Press the **tab key** on your keyboard until you see the link "**Continue to this website (not recommended)**"
2. Click on it.

Using the Extricom Web Configuration Pages

The Extricom Web Configuration pages have four main areas:

- Switch image – The Extricom Web configuration page displays an image of the configured switch (MS-500/1000) at the top of the page; the image shows dynamic status of the PoE of each AP port (grey = PoE off, green = PoE on).
- Navigation tree
- Configuration display, and editable work area (for some screens)

- Event and alarm area

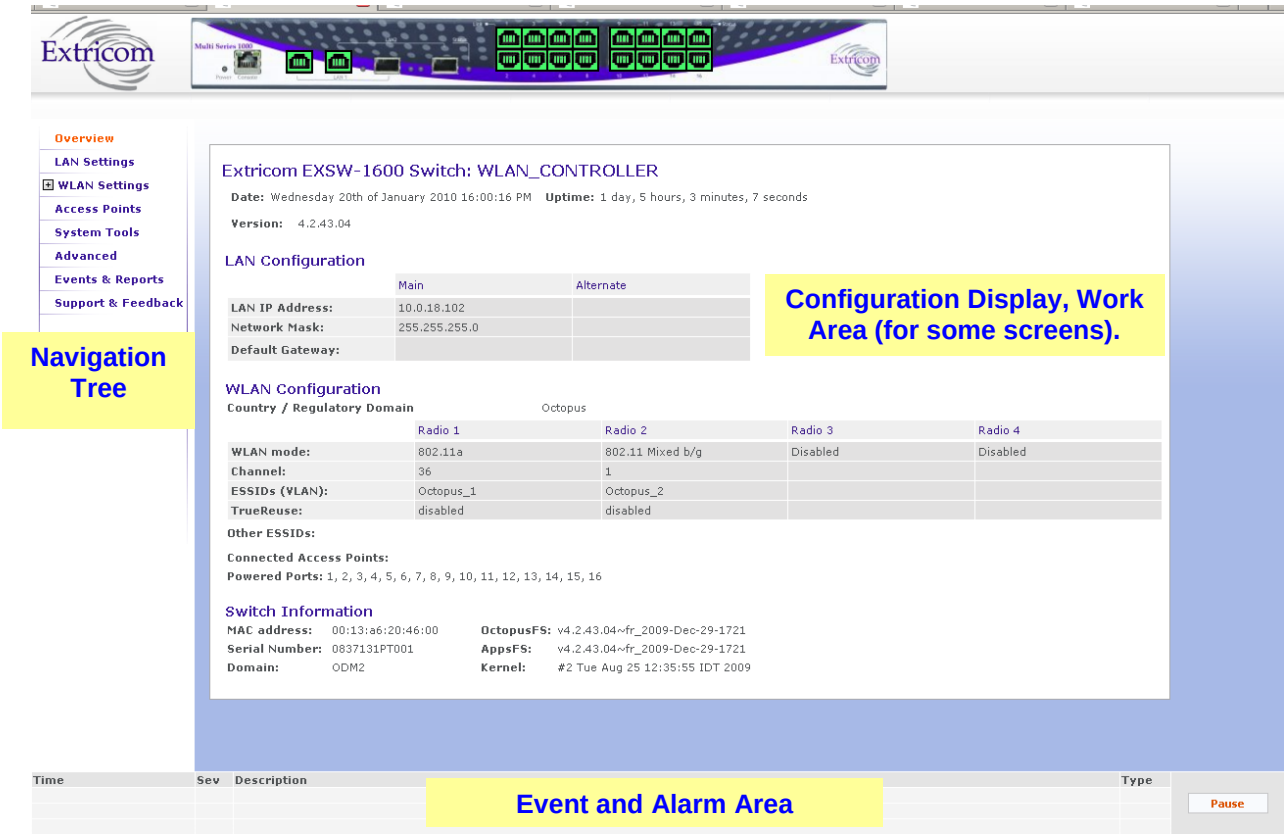


Figure 19: Typical Web Configuration Page

The *navigation tree* provides access to the *Overview* display, as well as the following Extricom Web configuration pages:

- Quick Setup - a wizard used to quickly set up a basic switch configuration.
- *LAN* Settings – used for configuring LAN parameters.
- *WLAN Settings* – used for configuring WLAN parameters including ESSID-related configuration and Radio configuration.
- *Access Points* – used for viewing ports in use, and activating/deactivating PoE.
- *System tools* – used for configuring general system parameters such as passwords, time & date, firmware upgrade, etc.
- *Advanced*– used for configuring advanced features such as redundancy, TrueReuse, 802.11d, IDS, SNMP, and Centralized Configuration parameters.
- *Events & Reports* – used for viewing system events and performance reports.
- Support & Feedback

The *work area* displays the configuration settings corresponding to the category selected in the navigation tree. Use this area to configure Extricom system parameters, where applicable. Web configuration pages may include a **Save** button; when this is selected, the configuration changes are applied to the offline configuration file. If you wish to apply these parameters, click **Apply System Tools** configuration section; this will start the reconfiguration process.

If you do not select **Apply** (in the **System Tools** configuration section) after clicking **Save**, the new configuration will only take effect after the switch is rebooted.

NOTE: If you change the IP address of the switch, and the new IP address is on the same subnet as the previous one, you will not lose the connection session. If however, the new IP address is on a subnet, different from the one your PC is on, the connection session will be lost. In this case, you will have to configure your PC with a new IP address that is in the same subnet with the switch and start a new http session.

The *event and alarm* area will display real time SNMP trap messages, you can pause the traps by selecting **Pause**.

Please see the Northbound SNMP Traps section for more details.

Configuring LAN Parameters

In the *LAN Configuration* page, you can configure the following:

- The LAN port's IP address along with the network mask, as well as a backup IP address with its network mask.
- The LAN interface and management VLAN tag IDs.
- The default gateway.

To configure LAN parameters:

- Click **LAN Settings** in the navigation tree. The *LAN Settings* page appears (refer to Figure 20).

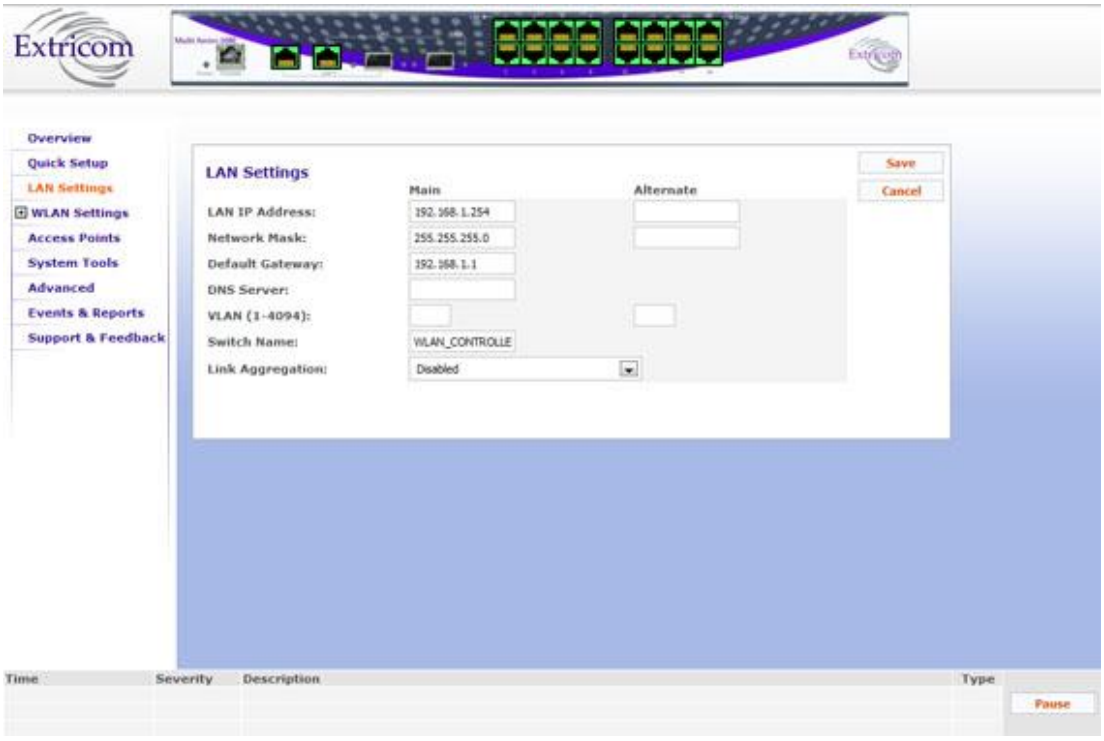


Figure 20: LAN Settings Page

- Configure the LAN parameters. Refer to Table 6 for a description of the LAN parameters.

Field	Description
LAN IP Address	LAN IP address used for the switch management. You may add an alternate IP address if you wish to manage the switch from a different network. In that case enter the value in the **Alternate** field.
Network Mask	Network mask for the LAN 1 IP address. You may also add an alternate network mask in the alternate filed for the alternate IP address defined.
Edge's Subnet	Subnet of a redundant pair (Primary - Secondary or Main - Standby). Only appears if the switch is defined as a part of a redundant pair, i.e. in a cascade configuration.
Default Gateway	IP address of the default gateway.
DNS server	IP address of the DNS server.
VLAN	Tag ID for VLAN used for the switch management. You may add two VLAN tag Ids: one for the LAN 1 IP address in the **Main** field, and an alternate one for the alternate IP address, using the **Alternate** field.
Switch Name	An alphanumeric descriptor of the switch. Maximum length is 64 characters.
Link Aggregation	A drop down menu with the following 6 options: 1. Disabled 2. Round-Robin Policy 3. Active Backup Policy 4. XOR Policy 5. Broadcast Policy 6. IEE 802.3ad Dynamic Link Aggregation

Table 6: LAN Configuration Parameters

- Click **Save** to save the configuration.

IMPORTANT! The changes made to the configuration will be lost, if you do not click **Apply** in the **System Tool**s configuration section after clicking **Save** on one or several configuration pages. Please refer to the Reboot section.

Configuring WLAN Settings

The *WLAN Settings* section is subdivided into three menu sub-sections:

- ESSID Definition
- Radios
- Assignments

Configuring ESSID Definition

An *ESSID* (Extended Service Set Identifier) is a name of a network, which is defined by a set of privileges, settings, and limitations (such as security definitions, access privileges, VLAN assignments, etc.) Each wireless device must connect to a specific ESSID. Each channel can support multiple ESSIDs, thus creating "virtual" networks on the same channel.

The following is the data structure used by the Extricom systems:

- Each radio is assigned one channel.
- Each channel can support up to 8 (or 16) different ESSIDs (see note below).
- Each ESSID can be associated with a VLAN tag.
- The same ESSID name can be repeated for different channels;

On the MS-500/1000, up to 7 ESSIDs are allowed on channel 1, and up to 8 ESSIDs are allowed on each of the remaining channels.

There is a maximum of 31 ESSIDs per system.

Table 7 below shows an example of possible channel, ESSID and VLAN tag assignments for the MS-500/1000 switches.

Access Point	Channel	ESSID	VLAN tag
First Radio	1	Network1	1
		Network2	2
		…	…
		…	…
		Network15	15
Second Radio	6	Network16	16
		Network17	17
		Network18	18
		…	…

Access Point	Channel	ESSID	VLAN tag
		…	…
		Network31	31

Table 7: ESSID per channel Example

In the *ESSID* web page, there are the following four configuration tabs:

- ESSID Settings
- MAC ACL
- MAC ACL Scheduler
- RADIUS

ESSID Settings

Under this tab you may **Add** a new ESSID, as well as **Rename** or **Delete** an existing ESSID. You may configure each ESSID by changing the following configuration parameters:

- Allow Default ESSID
- Display ESSID in Beacon
- Allow Store & Forward
- Allow Inter-ESS Store & Forward
- Enable Multicast
- Specify Multicast Rate Control
- Specify Broadcast Rate Control
- Enable MAC Authentication
- Enable MAC ACL
- Specify MAC ACL Mode
- Enable 802.11D support
- Enable ARP Caching
- Enable Bandwidth Saving ARP Caching
- Specify Beacon Rate Control
- Enable In Band Management
- Enable Captive Portal
- Assign a VLAN to the ESSID
- Set a Disassociation Timeout

- Select a DTIM period
- Enable EAPOL Start Only mode
- Select the Encryption method and set the parameters for it
- Select MAC Authentication RADIUS Server
- Select RADIUS Accounting Server

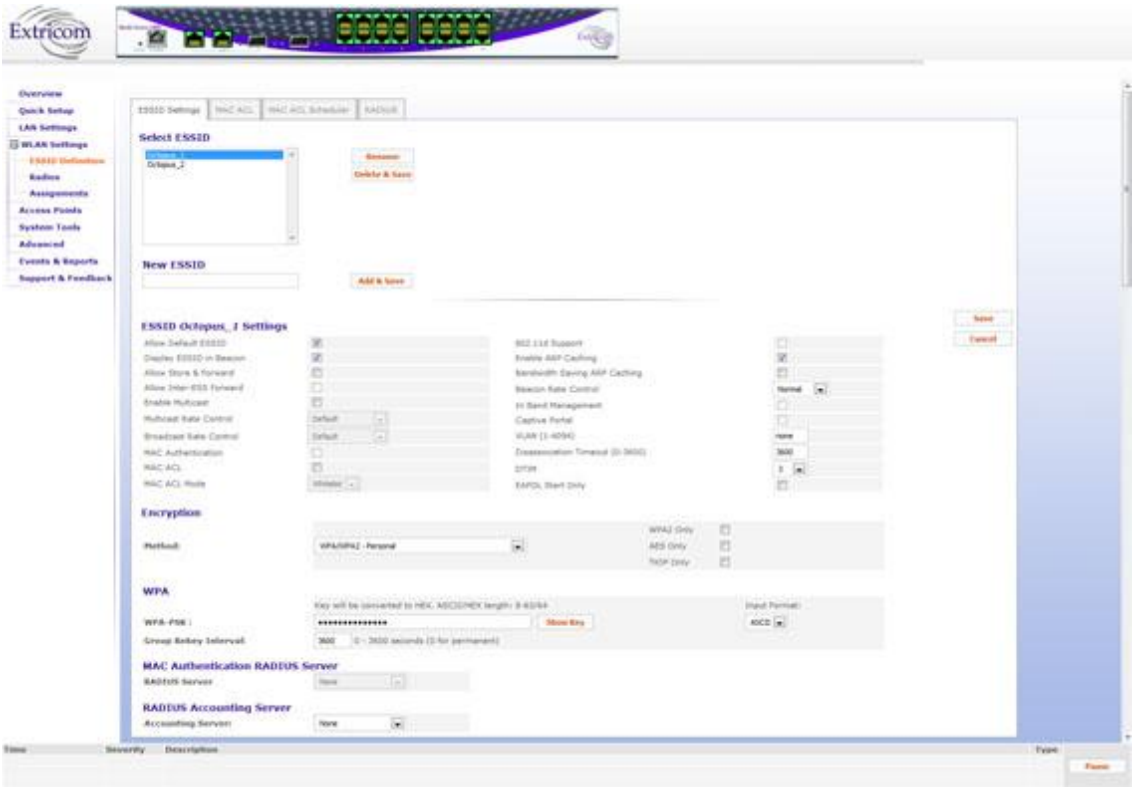


Figure 21: WLAN ESSID Definition Page - ESSID Settings Tab

When configuring ESSID parameters, refer to the following table for a description of the available parameters:

Field	Description
ESSID	
Select ESSID	Select an ESSID from the list. Once selected (highlighted), you may add **or** rename it by clicking on either the **Rename** or the **Delete & Save** button on the right.
New ESSID	Type in the new ESSID name string and click on the **Add & Save** button on the right.

Field	Description
ESSID <ESSID name> Settings	
Allow Default ESSID	If this option is *enabled*, a wireless device will be allowed to connect to the Extricom WLAN without requesting a specific ESSID (i.e., "default" or "any" ESSID). If this option is *disabled*, then a wireless device needs to connect to a specific ESSID in the Extricom WLAN.
Display ESSID in Beacon	This option provides an additional (though limited) level of security. The AP sends out a beacon with information about the network. If this option is enabled, the ESSID appears in the beacon. If disabled, the ESSID does not appear in the beacon.
Allow Store & Forward	If this option is *enabled*, two wireless devices connected to the Extricom WLAN with the same ESSID can communicate and transfer data to each other. Traffic between wireless devices will not be forwarded to the LAN switch. If this option is *disabled*, all traffic goes through the LAN switch. This could be used by IT managers to apply security settings or various policies on the LAN network. Disabling *Allow Store & Forward* disables the *Allow Inter-ESS Forward* option.
Allow Inter-ESS Forward	If this option is *enabled*, two wireless devices connected to the Extricom WLAN with different ESSIDs will be able to communicate with each other without going through a router. Traffic between wireless devices will not be forwarded to the LAN switch. This option must be enabled on both ESSIDs. In order for wireless devices, associated to different ESSIDs, to be able to communicate with each other, the ESSIDs must be defined on the same VLAN (or no VLAN at all). If this option is *disabled*, all traffic goes through the LAN switch. This could be used by IT managers to apply security settings or various policies on the LAN network.
Enable Multicast	This option, when enabled, provides support of multicast and broadcast packets for the selected ESSID. Multicast and/or broadcast packets shall be transmitted from all APs. Once this feature is enabled, Multicast Rate Control and Broadcast Rate Control may be left as default, or changed to Rate Optimized or Range Optimized.

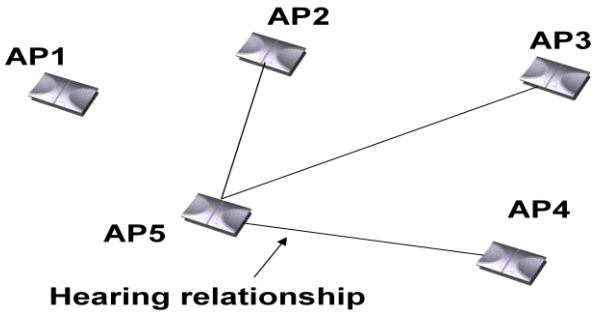
Field	Description
MAC Authentication	Select this option if you wish to impose MAC authentication on this ESSID. MAC authentication enables a user to authenticate WLAN clients using RADIUS server, even if they do not support 802.1 x authentications. Note that when using this option, the security setting does not allow you to select any 802.1x methods. [To enable this option go to "*Advanced →Others*" tab.]
MAC ACL	This option, when enabled, allows a user to add a MAC access list to the specific ESSID. Only clients with MAC address included in this list are allowed to access the network if the MAC ACL mode is set to Whitelist. Conversely, if the MAC ACL mode is set to Blacklist, then these clients are not allowed to use the network. [Use the MAC ACL tab on this page to add MAC ACL lists.]
802.11d Support	Enables support of the 802.11d standard. The purpose of this standard is to provide regulation domains for each country in a predefined list. The regulation domains and country information are provided as part of Beacons & Probe response. To use this feature, 802.11d support per ESSID must first be enabled [under the Others tab on the Advanced page].
Enable ARP Caching	This option, when enabled, provides an immediate response to ARP requests directed towards WLAN stations associated with the selected ESSID. The Switch answers on behalf of the WLAN stations. Note: ARP Caching is enabled by default.
Bandwidth Saving ARP Caching	Reduce the number of ARP packets sent over the wireless medium.
Beacon Rate Control	Use this option if you wish to tune the beacon distribution mechanism. You can tune the system to provide customized beacon coverage. The higher the rate, the more beacons shall be distributed on this SSID. For explanation of the Beacon Rate Control mechanism, see the section "Beacon Rate Control" below. Select one of the 5 rates available in the drop-down menu: • Basic: 0% beacon rate control • Normal (default): 33% beacon rate control • Increased: 66% beacon rate control • High: 80% beacon rate control • Full: 100% beacon rate control [To enable this option go to "*Advanced →Others*" tab.]

Field	Description
In Band Management	Select this option if you wish to allow management of the switch via the wireless media through this ESSID. In band management ESSIDs are assigned to the same VLAN as the VLAN which has been set up for the switch management. Once you set this option, the VLAN setting will be automatically updated to the management VLAN as set in the **LAN Configuration** web page. If in band management SSID is enabled, only the following security Settings are permitted (This should be set from the **Others Tab** on the **Advanced** page): • WPA/WPA2 personal (TKIP/AES & Pre Shared Key Authentication) • WPA/WPA2 Enterprise (TKIP/AES & 802.1x Authentication)
Captive Portal	Select this option if you wish to set this ESSID to be captive portal restricted. If you set this option the ESSID VLAN id is automatically assigned with the VLAN ID specified in the **Portal** tab in the **Advanced** page.
VLAN	Enter a VLAN tag to assign to the ESSID. Assigning a VLAN to an ESSID enables you to control a wireless device's privileges through the existing wired network definitions.
Disassociation Timeout	Enter the amount of time (in seconds) a wireless device can remain inactive (no data sent to or from the wireless device) before automatically disconnecting it from the network.
DTIM	The period of time after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. Select the DTIM period from the drop-down menu. This is relevant for clients that want to utilize the power management capability. The possible values are 1-5. The default is 3. A high DTIM value may cause these clients to lose connection with the network.
EAPOL Start Only	Select this option if you want the switch to only connect to clients that require the switch to wait for an EAPOL Start. When this option is selected, clients that do not send an EAPOL start will not be able to connect to this ESSID.

Table 8: ESSID Parameter Descriptions

Beacon Rate Control

The EXSW creates a hearing relationship table between APs. It forms an AP bundles group, where each bundle can include 1 or more APs. The total number of bundles is equal to the number of APs. Each bundle can send a Beacon at the same time interval. The transmission then occurs based on a round-robin principal, where every bundle transmits every 100msec. In order to compensate sensitive clients for a lost beacon, it is possible to set (per SSID) the Beacon rate control at a higher threshold. Although the feature minimizes the possibility of clients receiving duplicate beacons, there is no guarantee of zero duplicate/missed beacons.



*** Clients near AP1 hear only 1 beacon out of 5, therefore Hearing rate is 20%.**

Figure22: Hearing Topology Example

The following table shows the hearing rate (in %) of each AP in the diagram above:

AP	Receiving APs	Hearing Rate (%)
1	1	20
2	2,5	40
3	3,5	40
4	4,5	40
5	2,3,4,5	80

Table 9: Hearing Rate (%)

Beacon transmission prior to switch s/w v3.4 would have followed the legacy pattern below:

Bundle/Interval	BC1	BC2	BC3	BC4	BC5
1	AP1				
2		AP2			
3			AP3		
4				AP4	
5					AP5

Table 10: Legacy Pattern

However, beginning with v3.4, the Smart Beacon mechanism was implemented, so the beaconing in the example actually happens as shown in the table below (BC rate control of 80%):

Bundle/Interval	BC1	BC2	BC3	BC4	BC5
1	AP1,AP5				
2		AP1,AP2			
3			AP1,AP3,AP5		
4				AP5,AP4	
5					AP1,AP5

Table 11: Smart Beaconing

Configuring Security Definitions

In the *Encryption* section of the *ESSID Settings configuration* page the following security definitions can be configured:

- Method of encryption.
- Type of authentication.

With some configurations, you can use encryption without authentication. For a higher level of security, however, it is recommended to use both encryption and authentication. The Extricom WLAN makes configuration of ESSID security parameters easier by listing available combinations of Encryption and Authentication protocols.

Security definitions are configured for each ESSID individually.

To configure the security definitions:

1. Click on the ESSID for which you want to configure the security definitions in the **Select ESSID** field.
2. Configure the security definitions for the selected ESSID. Refer to Table 12 below for a description of Security parameters.

Field	Description
Encryption & Authentication	

Field	Description
Encryption	Choose the method of encryption with or without authentication. A combination of encryption and authentication methods may be selected from the **Method** drop-down list. There are eight options available: • N*one* – no authentication. • *WEP64*– Wired Equivalent Privacy (802.11 encryption protocol). This is a very basic encryption level. (AKA WEP40) • *WEP128*– This encryption is similar to WEP64, but the WEP keys are longer. (AKA WEP104). • *WEP64 & 802.1x Authentication* – WEP key is used for authentication and encrypting the data frames • *WEP128 & 802.1x Authentication* – analogous to WEP 64 & 802.1x Authentication, but with AKA WEP 104 • *WPA/WPA2 Personal* –Wi-Fi Protected Access/Wi-Fi Protected Access 2. Also referred to as WPA-PSK (Pre-shared key) mode, it is designed for home and small office networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase. • *WPA/WPA2 Enterprise*– Also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK). It is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). An Extensible Authentication Protocol (EAP) is used for authentication, which comes in different flavors. • *WPA/WPA2 - Enterprise & Personal* enables the wireless client to choose from either of the two methods on a single ESSID. In addition, there are three types of **encryption ciphers** available: • *WPA2 - Wireless Protected Access 2, the Wi-Fi alliance certification of 802.11i that uses CCMP/AES encryption.* • *AES* – Advanced Encryption Standard.(Cipher Block Chaining Message Authentication Code Protocol) is currently the most advanced and secured method of Wi-Fi encryption and is part of 802.11i (WPA2) standard. • *TKIP* – Temporal Key Integrity Protocol. This is a more secure and more advanced method of encryption as a part of the WPA standard. When the “WPA2 Only” is checked, only Clients with WPA2 support are allowed to access the WLAN. When the “AES Only” is checked, only Clients with AES support are allowed to access the WLAN. Cisco LEAP protocol (not CMIC & CKIP) is supported under “*WEPxxx & 802.1x Authentication*”.

Authentication method

Authentication is used to identify if a wireless device is authorized

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>WEP Keys</td><td>The WEP Keys area is only enabled if the cipher selected in the Method field of the Encryption area is either WEP64, WEP128, WEP64 & 802.1X Authentication, or WEP128 & 802.1X Authentication. In the WEP Keys area, you define the WEP Transmission Key that is used for encrypting or decrypting. You can define all four WEP keys. For the transmission key you define, select the input format (ASCII or HEX) and enter the key according to the following table:
<table>
<tr><th>Cipher</th><th>ASCII</th><th>HEX</th></tr>
<tr><td>WEP64
(or WEP64+802.1x)</td><td>5 characters</td><td>10 digits</td></tr>
<tr><td>WEP128
(or WEP128+802.1x)</td><td>13 characters</td><td>26 digits</td></tr>
</table>
</td></tr>
<tr><td>WPA</td><td>The WPA area is only enabled if the cipher selected in the Method field of the Encryption area is either WPA/WPA2 Personal, WPA/WPA2 Enterprise, or WPA/WPA2 Personal & Enterprise.
If WPA/WPA2 Personal or WPA/WPA2 Personal & Enterprise with Pre-Shared key authentication method is used, the WPA-PSK field is enabled. In this case, select one of the following input formats, and enter the corresponding key listed:
• For ASCII, enter 8-63 characters.
• For HEX, enter 64 digits.
You may select to either show or hide the key characters by either pressing Show Key or Hide Key button to the right of the Key field.
For all WPA/WPA2 encryption methods you may specify Group Rekey Interval, which is the amount of time (in seconds) that elapses before the Group Key is changed.</td></tr>
<tr><td>MAC Authentication RADIUS Server</td><td>This configuration option becomes available if the WEP64 or WEP128 encryption method is selected. Define the MAC Authentication RADIUS Server by selecting one from the drop-down list.</td></tr>
</table>

Field	Description
RADIUS Authentication Servers	Define the RADIUS Authentication Server(s) by selecting one (or more, up to four) from the drop-down list if: • The WEP64/WEP128 encryption with the 802.1x authentication method is selected, or • The WPA/WPA2 - Enterprise or WPA/WPA2 - Enterprise & Personal authentication method with the TKIP/AES cipher is selected. Use Server # 1 if only one server is used. Use consecutive servers if several servers are used.
RADIUS Accounting Server	Select the RADIUS accounting server from the drop-down list of RADIUS servers.

Table 12: Security Definition Parameters

Configuring MAC ACL

To configure a per-ESSID MAC ACL, select the MAC ACL tab in the ESSID Definition configuration screen.

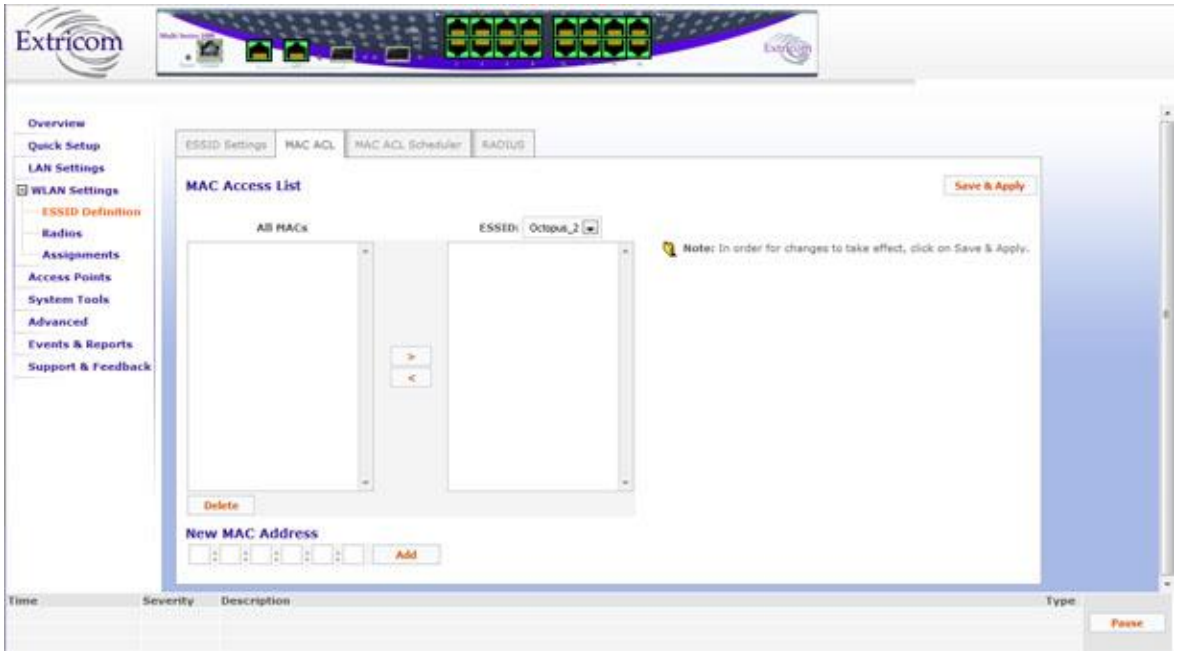


Figure 23: MAC ACL Configuration Tab

1. Select one of the configured ESSIDs from the **ESSID:** drop-down list.
2. Select a MAC address from the list in the **All MACs** field.
3. Use the right arrow to add this MAC address to the **ESSID:** field (use the left arrow to remove a MAC address from the **ESSID:** field).

4. You may add a new MAC address to the **All MACs** list by inserting it manually in the **New MAC Address** field, then clicking **Add**. It is also possible to add a new MAC address to the **All MACs** table from the Event Menu. When a new event message notification appears, informing you of a new client it will have a + button in the **Add** field. Once you click this button, the MAC address of the new client is automatically added to the **All MACs** list.
5. You may also remove a MAC address from the **All MACs** list by highlighting it and clicking **Delete** below the **All MACS** field.
6. Click **Save & Apply** to save the configuration and apply it immediately. There is no need to use the main Apply page.

Configuring MAC ACL Scheduler

The MAC ACL scheduler allows you to customize ACL configuration to allow various ACLs be activated at various times. To schedule ACL tasks, select the **MAC ACL Scheduler** tab in the ESSID Definition configuration section.

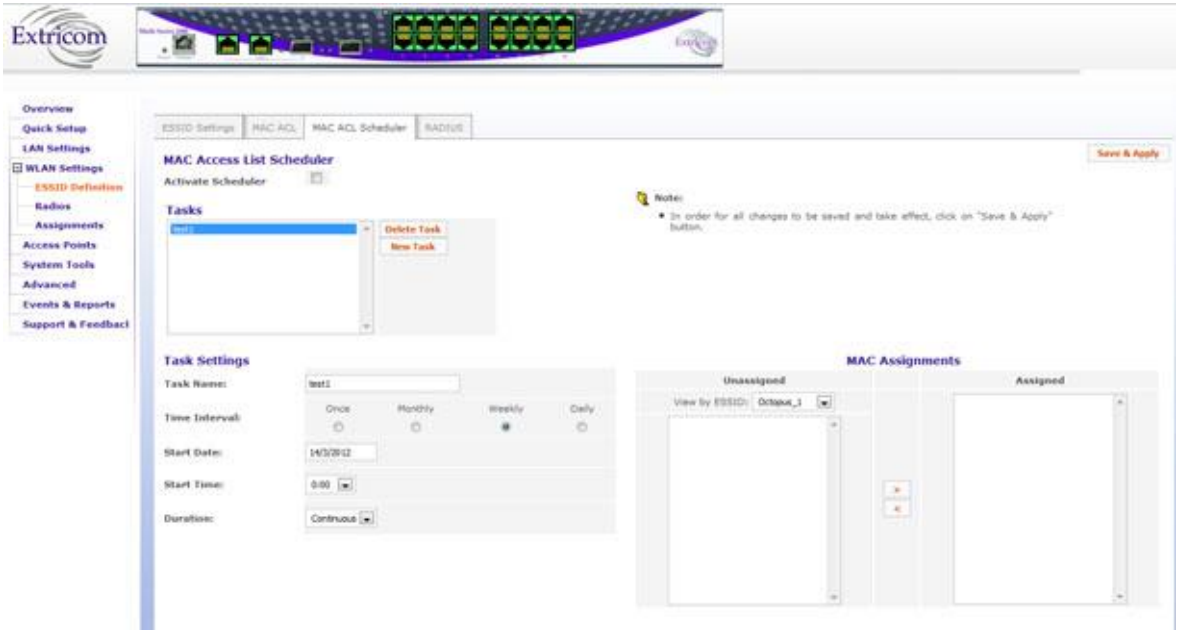


Figure 24: MAC ACL Scheduler Configuration Tab

MAC ACL schedule may be activated by selecting the **MAC Access List Scheduler** checkbox at the top of the work area. Further,

1. To add a new ACL schedule, click **New Task**. An entry named *New Task* will appear in the **Tasks** field. You may also delete a schedule by selecting it from the list in the **Tasks** field and clicking **Delete Task**.
2. To configure the newly added schedule, or to modify an existing one, select it from the list in the **Tasks** field, then proceed to the **Task Settings** area of the configuration, as described in the table 14 below:

Field	Description
Task Name	Assign a name to a selected schedule by entering an alpha-numeric string in this field.
Time Interval:	You may assign periodicity of an ACL by selecting one of the following radio buttons: • Once • Monthly • Weekly • Daily
Start Date	Click inside the date field and navigate to the desired start date in the pop-up calendar.
Start Time	Select the start time from the drop-down menu. The options are in the range from 0:00 to 23:00 in increments of one hour.
Duration	Select the time interval during which the ACL will be activated. The values in the drop-down menu are "Continuous", "1 hour", "2 hours", etc. through "24 hours".

Table13: MAC ACL Scheduler Parameters

3. To apply selected ACL task to specified MAC addresses, proceed to the **MAC Assignments** area of the configuration screen. Here you may move various MAC addresses between the **Unassigned** and **Assigned** fields by using the left and the right arrow keys. You may either display all ACLs or only those associated with specific ESSIDs by selecting the specific ESSID or "all" from the *Viewed by ESSID* drop-down menu.

Configuring RADIUS

To configure the RADIUS server option, select the RADIUS tab in the ESSID Definition configuration section. The **RADIUS Servers** work area displays the already configured RADIUS servers in the system RADIUS server bank. Here, you may also configure new RADIUS servers, as well as delete entries that are no longer needed.

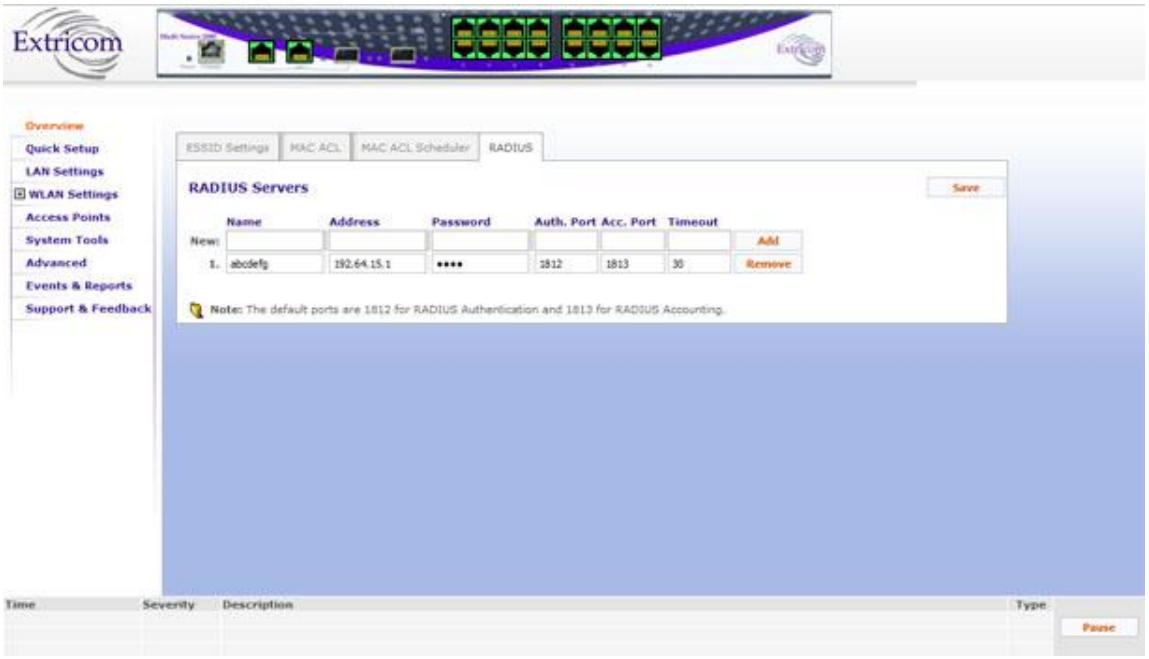


Figure 25: RADIUS Configuration Tab

1. You may remove a RADIUS server from the list by clicking **Remove** next to the server definition line.
2. To modify an existing server, or to configure the new one, specify the following parameters as outlined in the Table14 below:

Field	Description
Name	An ASCII string for the name of the RADIUS server.
Server Address	The IP address of the RADIUS server.
Password	The RADIUS server password.
Auth. Port	RADIUS authentication port number. The default value is 1812.
Acc. Port	RADIUS accounting port number. The default value is 1813.
Timeout	The time (in seconds) during which the Extricom switch will wait for the RADIUS server response, before it stops transmitting and switches to the next failover Radius server (if configured).

Table14: RADIUS Configuration Parameters

To save the configuration click **Save**. At the end you have to apply the configuration in the system tool section.

Configuring WLAN Radios

To configure the WLAN radios, select *Radios* under WLAN Settings in the navigation tree. On this configuration page you will find the following three configuration tabs:

- WLAN Wizard
- Radios
- WMM

Configuring Radios Using WLAN Wizard

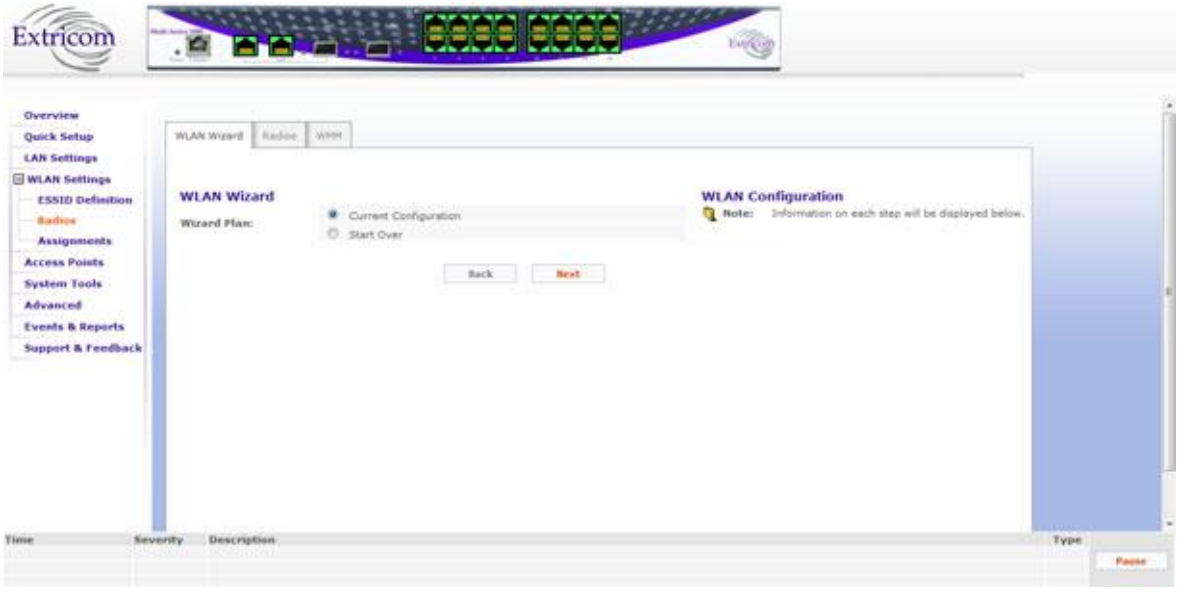


Figure 26: WLAN Wizard Configuration Page

Using the step-by-step **WLAN Wizard** facility, and starting with either the **Current Configuration** or a new one (**Start Over**), you may simplify the process of configuring the Radios, following the 5 pre-determined steps below.

1. *Access Point Type*.
2. *Rogue AP Detection Blanket.*
3. *Blanket Types*.
4. *TrueReuse*.
5. *Additional Parameters*.

At each step, a corresponding entry is displayed on the right-side of the configuration screen. For the details on the configuration parameters, refer to the Table 15 below.

Configuring Radios Manually

To configure each radio manually, click on the *Radios* tab to get to the Radios configuration screen.

When the Radios page is initially displayed, it appears in its abridged form. To see all of the configuration options, you must click on the "More Options" button. The window as shown in Figure 27 below appears.

> Note that when configuring 802.11a/b/g radios, the 802.11n displayed parameters cannot be configured and are grayed out.

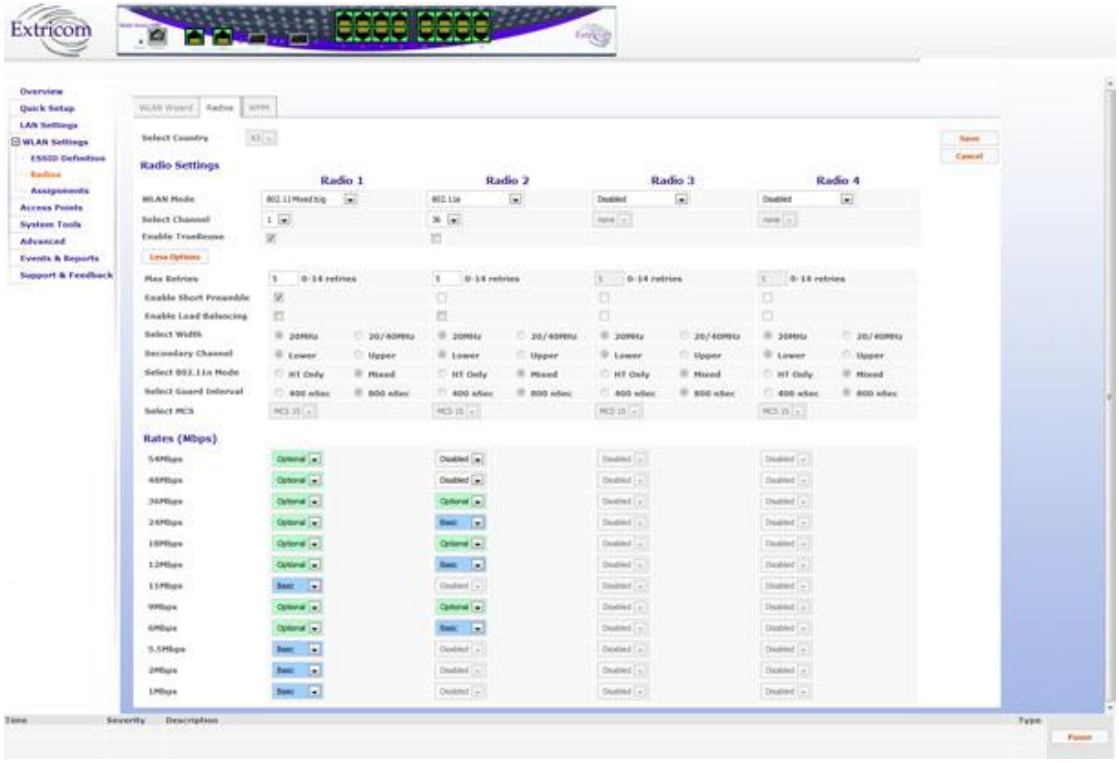


Figure 27 - Radios Configuration Page

The configuration parameters of each radio are arranged in a column. There are four columns, each of which is clearly identified with the corresponding title, i.e. **Radio 1**, **Radio 2**, etc. Refer to the Table 15 below to set up the configuration parameters.

Field	Description
Channel Options	
WLAN Mode	Select the WLAN mode from the drop-down menu. Possible options are: • Disable - choose this option to disable the radio • 802.11a • 802.11b • 802.11g • 802.11 Mixed b/g • 802.11n/a • 802.11n/g • 802.11n/g/b • Rogue detection Not all Same Band configurations are possible, depending on type of Access point connected, the configured radio state and whether TrueReuse is configured across the switch. See the Release Notes for possible configuration scenarios.
Select Channel	Select the channel from the drop-down menu. The options available are based on the country and WLAN mode.
Enable TrueReuse	Enable the TrueReuse function on the selected radio. Not all TrueReuse configuration scenarios are available. This depends on what Bands are configured on all other radios, the type of access point in use and the configured Radio state. See the Release Notes for possible configuration scenarios.
More/Less Options	Click this to hide or reveal additional configuration options.
Max Retries	Select the number of times that the switch tries to resend a packet if the transmission of that packet fails. Available values are 0 to 14.
Enable Short Preamble:	This option becomes available only when **802.11b** is selected as the WLAN mode. In this case, mark the checkbox to allow a short preamble.
Enable Load Balancing	Check this box if you want to enable load balancing. It is advised to connect mobile devices to the BSSID that is the least loaded one among all BSSIDs sharing the mobile devices' SSID. The number of connected users defines the metric that is used to determine the load.

Field	Description
The following parameters are available if one of the 802.11n-WLAN modes has been selected.	
Select Width	Check the appropriate radio button to select the width of the 802.11n channel , either 20MHz or 20/40MHz.
Secondary Channel	If 20/40MHz channel width is selected via the **Select Width** option, the system automatically configures the second 20MHz channel to be used for bonding as either above (Upper) or below (Lower)the primary 20MHz channel.
Select 802.11n Mode	Two blanket operational modes are supported: • **Mixed –** In this mode, the Channel Blanket is available to all WLAN clients, i.e. operating in 802.11a, 802.11b, 802.11g, etc modes. • **HT Only –** In this mode, the Channel Blanket is available to 802.11n clients only. Note that in this mode, the 802.11n devices are in fact working in a mixed mode, but the switch will not allow a/b/g devices to connect.
Select Guard Interval	Guard interval can be configured to short (400 nanoseconds) or long (800 nanoseconds). Note that when a 20MHz channel is configured, it is not possible to configure short guard interval.
Select MCS	Selecting the MCS is equivalent to setting the rate in legacy radios; MCS 0-7 use one data stream, while MCS 8-15 use two data streams.

Field	Description
802.11a/b/g Rate Configuration	**Data rate configuration is only applicable to 802.11a/b/g Channel Blankets**. For each of the data rates listed, select whether the rate is *Basic*, *Optional*, or *Disabled*. When configuring the data rates, you should consider the data rate capabilities of the wireless devices in your enterprise. • *Basic* – The *Basic* data rates are usually the data rates that the vast majority of your wireless devices can support. Only wireless devices that support all the *Basic* data rates will be connected to the WLAN system. Therefore, it is recommended that you configure a minimal number of *Basic* data rates that the vast majority or all your wireless devices can support. When working in Mixed Mode, there should be at least one *Basic* data rate from the 802.11b rates. • *Optional* – If you configure a data rate as *Optional*, the network will provide that data rate to wireless devices that can support it. • *Disabled* – *Disabled* data rates are not available to wireless devices. Since the Extricom WLAN system allows for dense deployment of APs, it is recommended, where applicable, to disable low data rates. Not doing so could possibly lead to an "edge user" effect, in which a client reduces aggregate network throughput by moving to the edge of the coverage area.

Table 15: Radio Configuration Parameters

Configuring WMM

To configure WMM, click on the *WMM* tab.

Note: WMM is configured per radio.

1. Select the radio from the drop down list.
2. Enable WMM by selecting the **Enable WMM** checkbox.
3. Configure the appropriate WMM parameters as described in the Table 16 below.

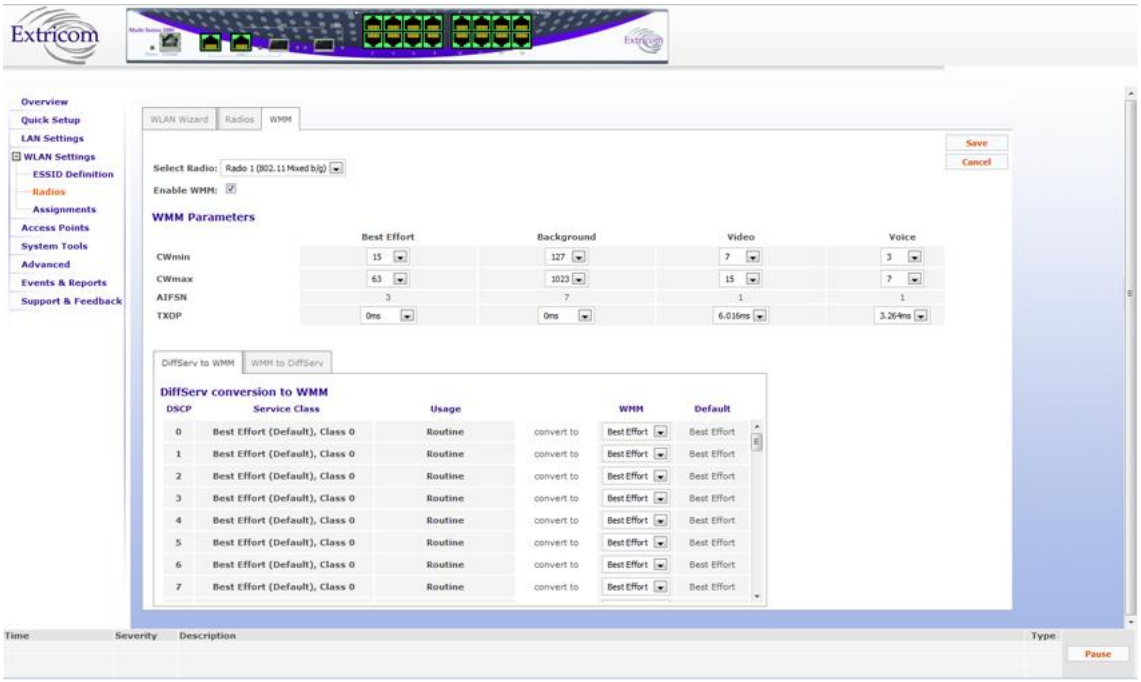


Figure 28: WMM Configuration Tab

Field	Description
CWmin	From the drop-down menu, select Min Contention Window (time slots) for each access category. Available values are: 3, 7, 15, 31, 63, 127, 255, 511, 1023. The default values for the following categories are: **Voice –** 3 **Video** – 7 **Best Effort** – 15 **Background** – 127
CWmax	From the drop-down menu, select Maximum Contention Window for each access category. Available values are: 3, 7, 15, 31, 63, 127, 255, 511, 1023. The default values for the following categories are: **Voice –** 7 **Video** – 15 **Best Effort** – 63 **Background** – 1023
AIFSN	Arbitration Inter Frame Spacing Number - predetermined and fixed for each Access Category and may not be changed.
TXOP	Interval (in milliseconds) during which a station can send as many frames as possible. Available values are: 0, 1.504, 3.008, 3.264, 6.016

Table 16: WMM Parameters Description

DiffServe conversion to WMM is mapped at the bottom of the configuration screen, under the **DiffServ to WMM** tab. The Table 17 below shows the default mapping of DSCP classes to WMM service classes:

DSCP Service Class	WMM Service Class
1 2	Background
0 3	Best Effort
4 5	Video
6 7	Voice

Table 17: IP priority To WMM Access Category mapping

The WMM values may be changed by selecting alternative ones from the drop-down menus under the current tab. The default mappings may also be changed by using the pull-down menus that appear under the **WMM to DiffServe** tab,

0x08	Background
0x20	
0x28	Video
0xa0	
0x30	Voice
0xe0	
0x88	
0xb8	
Other	Best Effort

Table 18: ToS To WMM Access Categroy mapping

ESSID Assignment

To assign specific radios to individual ESSIDs, select *Assignments* under WLAN Settings in the navigation tree.

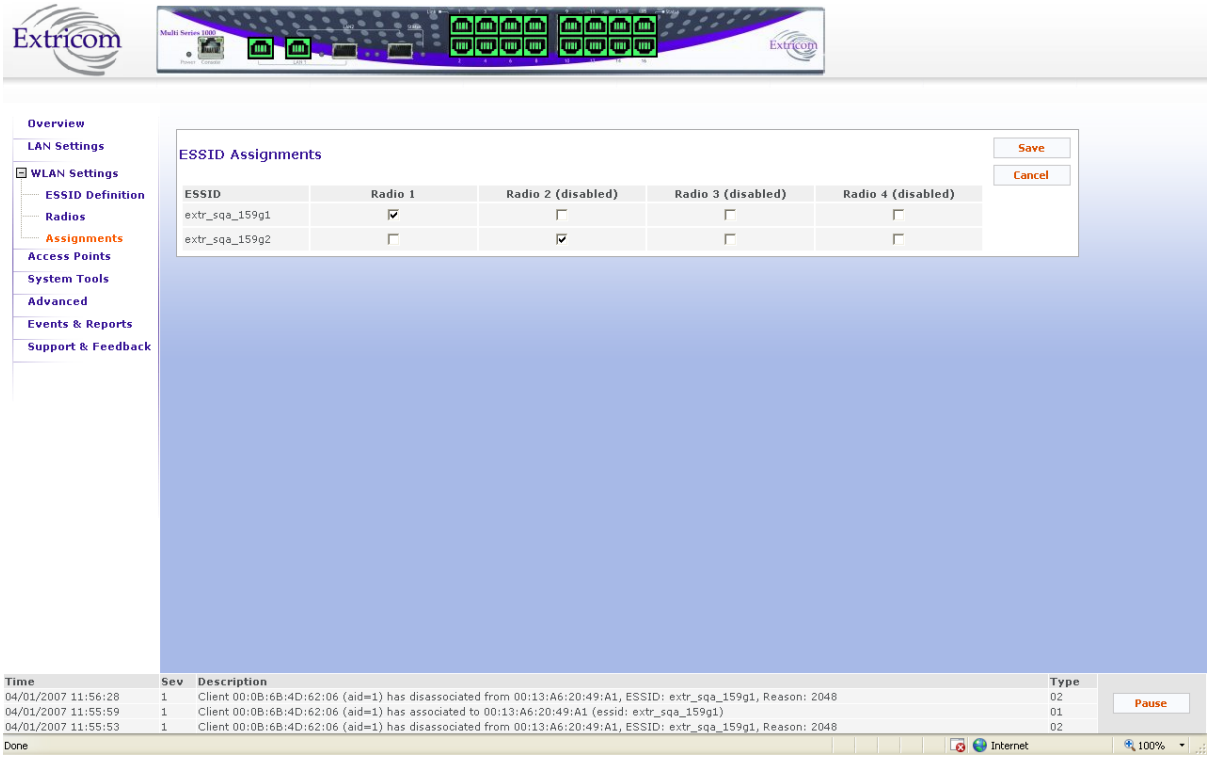


Figure 29: ESSID Assignment Page

The web page displays a cross-reference table of previously defined ESSIDs and Radios (1 to 4). Check the box for each ESSID you wish to assign to any of the four radios.

Powering Access Points

The only AP configuration required in the Extricom WLAN architecture is powering of the AP ports on or off.

To configure AP PoE status:

- Click on *Access Points* in the navigation tree. Under *PoE & Radio Controls* tab:
- Toggle an individual AP PoE on or off by clicking on its RJ45 connector image. The RJ45 connector image will turn either green or grey depending on whether it has been powered on or off respectively. To immediately activate your selection, click the **Apply** button on the right side of the configuration screen.
- An image of an AP connected to the RJ45 connector will appear if an AP is powered-on and connected to the port.
- To power on all of the APs with PoE, click the **Power on all** button on the right side of the screen.
- To power off all of the APs with PoE, click the **Power off all** button on the right side of the screen.

Note: the image of the switch on top of the page also color illustrates the PoE status of the APs.

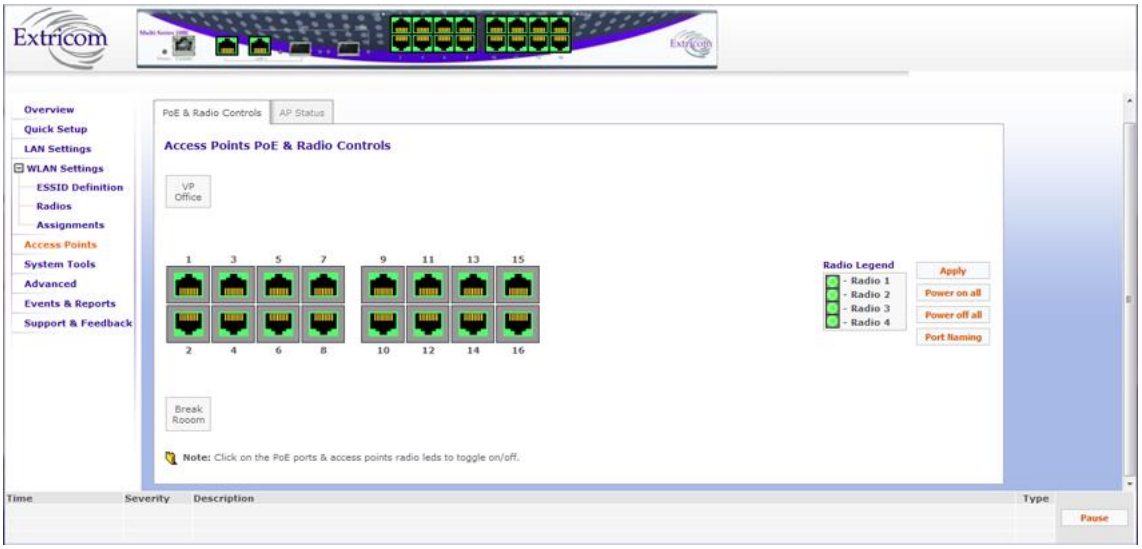


Figure 30: Access Points PoE & Radio Controls Page

You may choose to assign names to the ports. If you do, click the **Port Naming** button on the right side of the screen. The window will pop up.

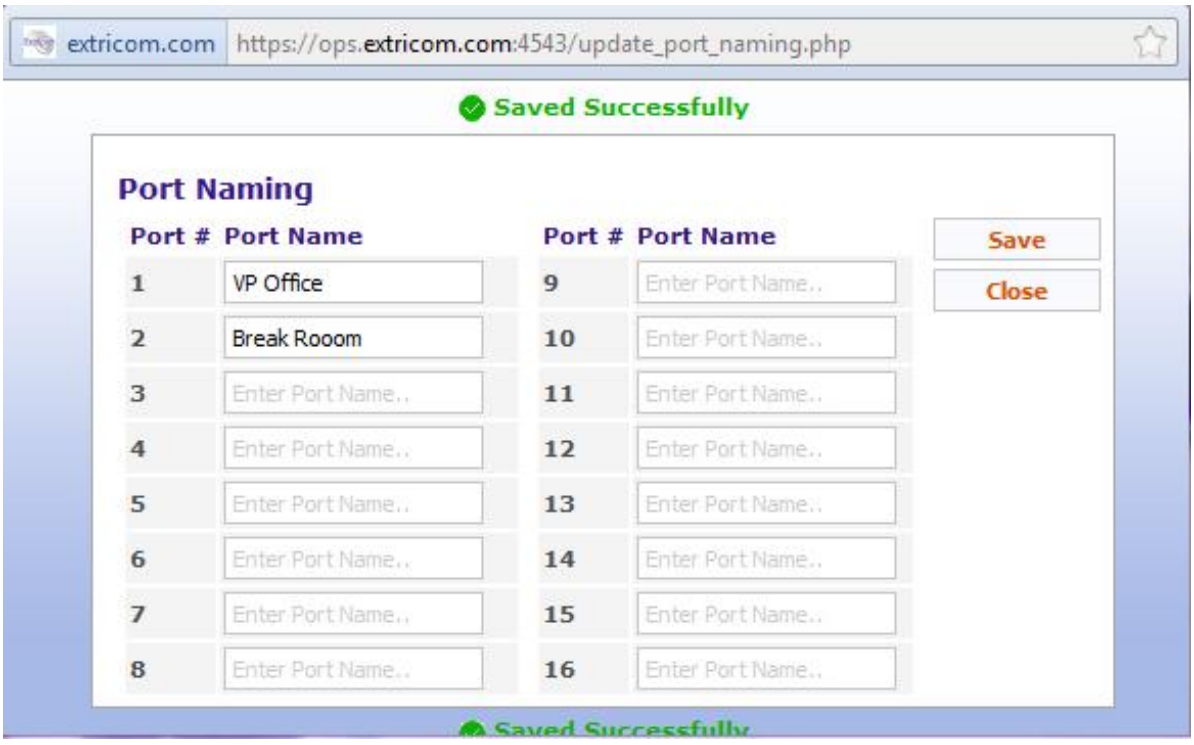


Figure 31: Port Naming Screen

Type in the names for the ports, then click **Save**, and **Close**.

To see which ports of the AP are up or down, click on the *AP Status tab*. To display the most up-to-date information, click on the **Refresh** button on the right.

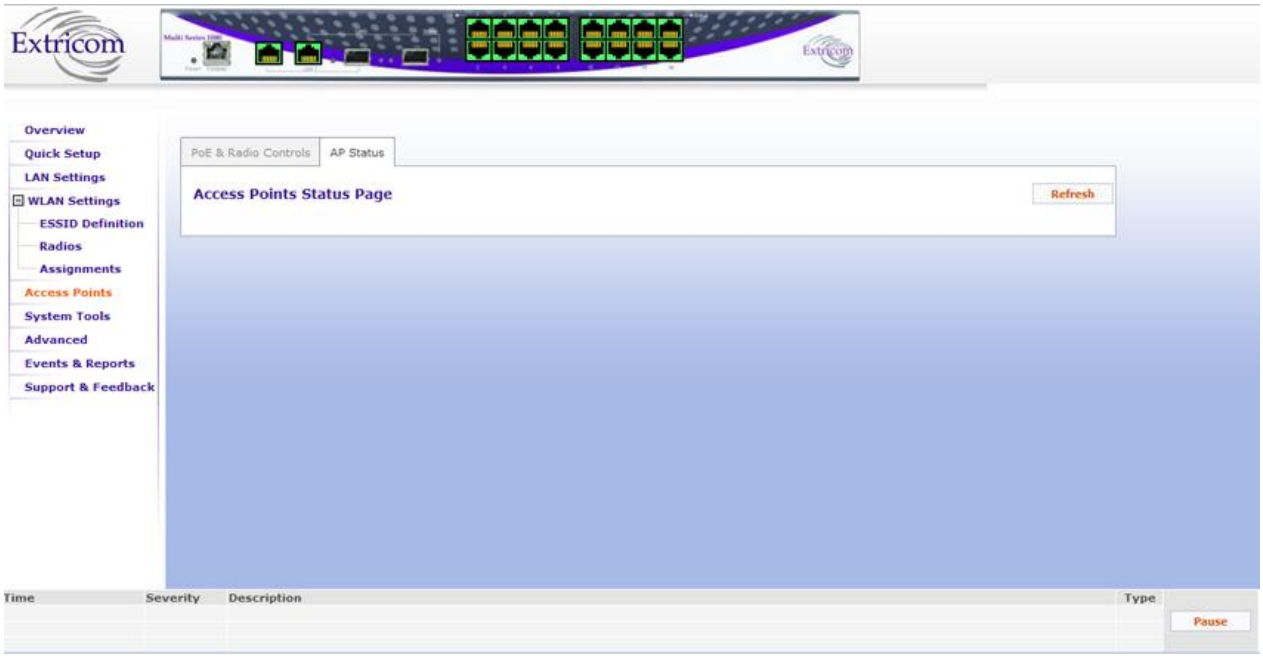


Figure 32: Access Points Status Page

Cascaded APs

When two switches have been cascaded together as Primary and Secondary (see Chapter 1, Switch Cascade section, for details about Switch Cascade configuration) the Access Point window is somewhat different. A tree of the two switches appears on the left to allow the user to easily toggle between views of the APs of each cascaded switch. The secondary switch is shown below the primary one in the tree:

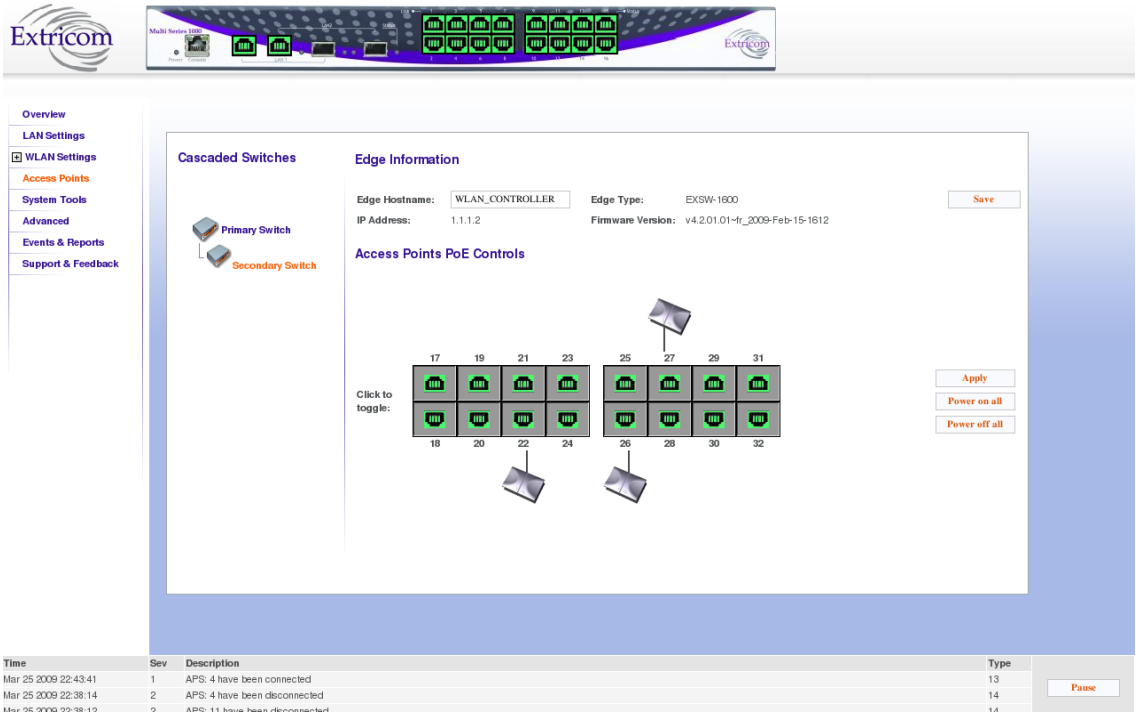


Figure 33: Access Point Configuration Window - Secondary Switch

System Tools Configuration

- This configuration section includes the following system tools tabs:
- Apply
- Reboot
- Maintenance
- Time & Date
- Passwords
- Upgrade
- Certificate
- Application
- License

Apply

Use this tab to apply the new configuration changes. Not every change in the configuration of an Extricom switch requires system reboot. Some parameters can be changed, and the changes will take effect immediately. The **Apply** button checks whether a full reboot is required. In case a reboot is not required, the updates will take effect immediately.

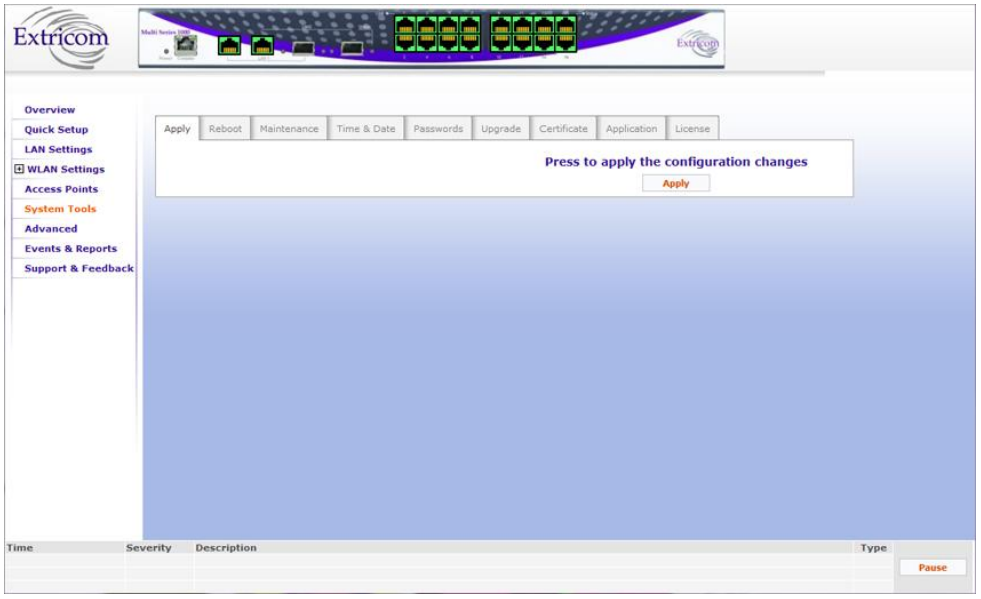


Figure 34: System Tools Configuration Page

Reboot

Use this tab to reboot the system. In some cases, such as upgrading/downgrading the firmware, or returning the Switch Cascade from failover to normal operation, a system reboot is required. Refer to the specific configuration update sections to see if the reboot is needed in order for the changes to take effect.

> ***A switch reboot will cause a temporary loss of WLAN service until the reboot process is complete.***

To reboot the Extricom switch:

1. Select the *Reboot* configuration tab and click **Reboot**.
2. A new screen opens, prompting you "Are you sure you want to reboot?"
3. Click **Reboot** to proceed.

> **Note**: Rebooting before applying OR saving the changes will discard those changes

Maintenance

Use the tab to:

- Save the current configuration to a disk.
- Upload a configuration to the switch.
- Restore the switch to factory default configuration.
- Undo configuration changes and return to the last applied configuration.

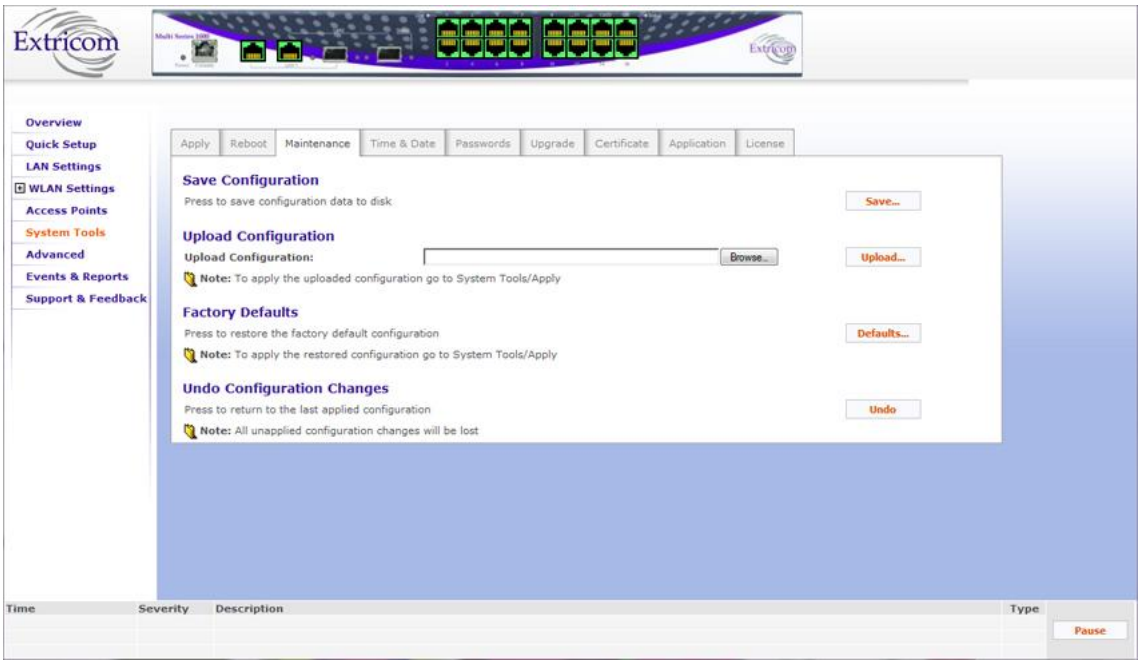


Figure 35: Maintenance Configuration Tab

Field	Description
Save Configuration	Save the active configuration to an offline disk.
Upload Configuration	Upload a configuration from an offline disk to the switch. Use the browse field to locate the configuration file. You will see a popup window stating "Please select configuration elements to upload"; you can select a *Switch*, a *MAC ACL*, or an *Allowed ESSID* configuration file.
Factory Defaults	Restore factory default configuration. You will see a popup window stating "Please select configuration elements to upload". You can select a *Switch*, a *MAC ACL*, or an *Allowed ESSID* configuration file, and/or Captive Portal Custom page.
Undo Configuration Changes	Return to the last applied configuration. All unapplied configuration changes will be lost.

Table 19: Maintenance Configuration Tab

To save the active configuration, click on the **Save** button, and specify the off-line location where you wish to save the file.

To upload a configuration, check the appropriate configuration elements in the “Browse” popup window, then click **Upload**:

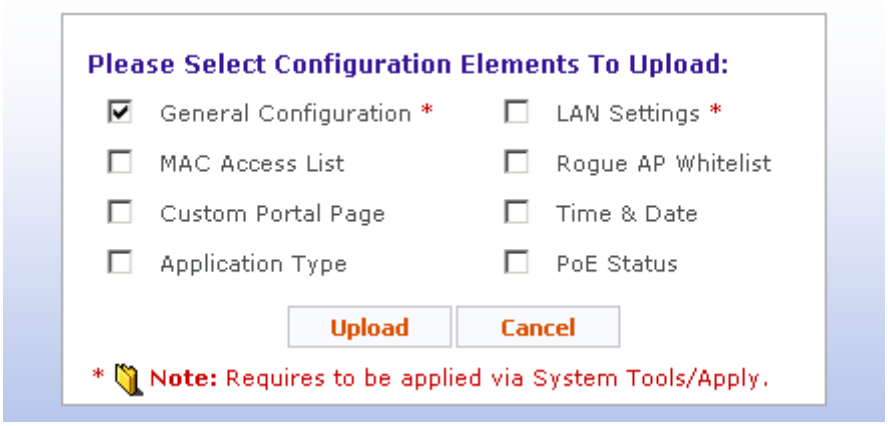


Figure 36: Pop-up Window - Configuration Elements to Upload

To restore the factory default parameters, check the appropriate boxes in the “Browse” popup window, then click **Restore**:

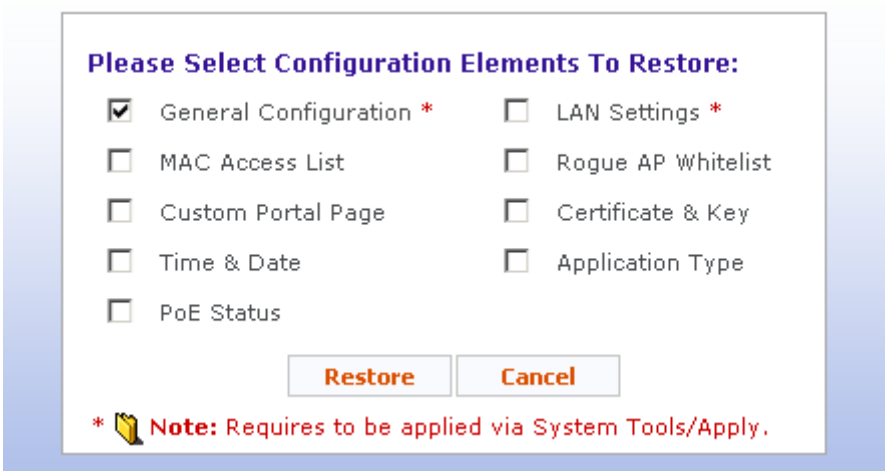


Figure 37: Pop-up Window - Configuration Elements to Restore

Time & Date

Use this configuration tab to set the time and the date on the switch. The Extricom system supports two ways of setting the time and the date - manual and using NTP protocol.

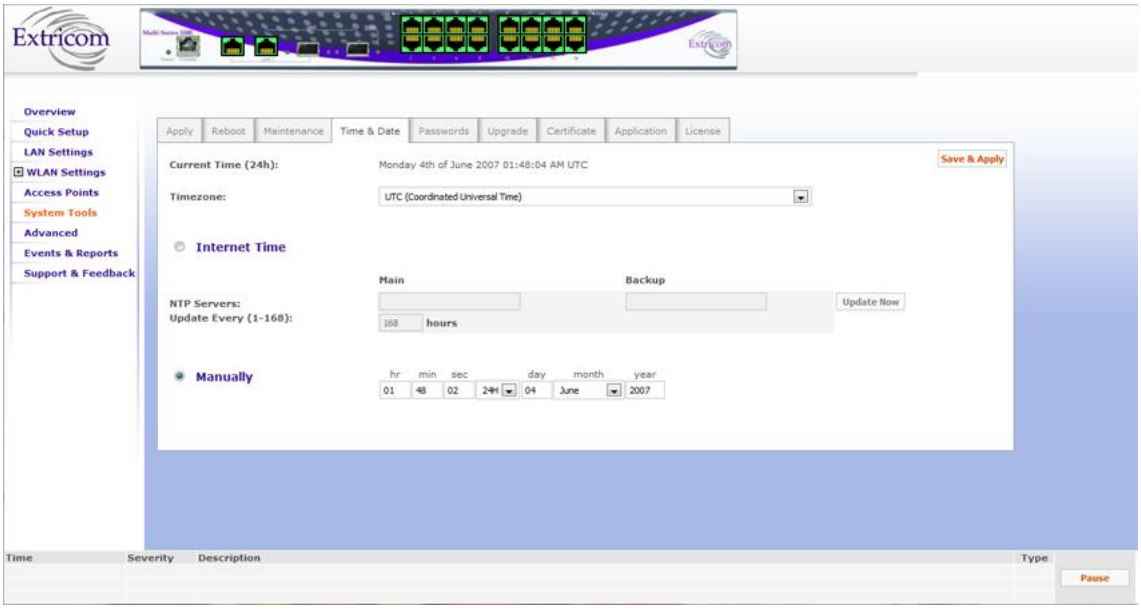


Figure 38: Time & Date Configuration Tab

To manually set the time and the date on your Extricom Switch:

1. Select the **Manually** radio button.
2. Enter the time and the date in the corresponding fields.
3. Click **Save and Apply**.

To set the time and the date on your Extricom Switch using NTP protocol:

1. Select the **Internet Time** radio button.
2. Select the **Timezone** from the drop-down menu.
3. Select the Main and the Backup NTP Servers. (Check the radio button next to the **Main** NTP server menu and select the **NTP server** from the drop-down menu. Repeat the procedure for the Backup NTP server).
   You may also specify Custom Main and Backup servers by entering their IP addresses in the **Custom Server IP:** fields.
4. Specify the NTP update interval (in hours) in the **Update Every (1-168):** field.
5. Click **Save and Apply** to immediately start the NTP process.
6. Click **Update Now** to synchronize the system clock with the NTP server.

Passwords

Use this tab to set or to change the passwords. Passwords are set according to the user access privileges. Refer to the Table 20 for default passwords according to the user access levels.

User Access Level	Privileges	Default Password
admin	Accessing the Web configuration.	Switch1
lobby	Accessing the Lobby administration page, which enables configuring new user.	Lobby (must be updated during initial use)
operator	User account , SSH access	12345
root	Super user	octopus

Table 20: Default Passwords

The "operator" and "root" passwords are used when accessing the switch for maintenance and service purposes. Changing these passwords should be performed only by an Extricom-authorized engineer.

For security purposes, it is important that all the passwords (including operator and root passwords) be changed from the default values when the switch is first installed, as well as periodically updated.

Record all passwords and store them in a safe location.

To set and change a password on an Extricom switch:

1. Select the **Passwords** tab.
2. Select the user category from the drop-down list.
3. Enter the current password.
4. Enter the new password.
5. Retype the new password.
6. Click **Apply**.

Upgrade

Use the *Upgrade* tab to upgrade the Extricom switch firmware as follows:

1. Download the upgrade file to your computer from the CD supplied with your purchase.
   or
   Obtain an upgrade file from your authorized Extricom reseller or distributor.
2. Create a backup of the current configuration as described under the Save option of the Maintenance configuration section.
3. Select the *Upgrade* tab, then click **Browse** and navigate to the location of the firmware upgrade file. The file's name with full path appears in the **Upgrade File** field.
4. Click **Upgrade** to upgrade the firmware and wait for the upgrade process to end. A message asking you to reboot the switch will appear once the upgrade is complete.
5. Reboot the switch as described in the Reboot configuration tab section above.

The firmware upgrade file is GNU zipped (gzip). Some Internet browsers are configured to automatically unzip files when downloading. Verify that this function is disabled so that the upgrade file remains zipped after downloading.

Upgrading a Switch Cascade pair is done via the primary switch GUI.

Certificate

The first time that a Captive Portal user logs in from his/her browser, he/she will receive a notice about a problem with the switch security certificate such as "There is a problem with the website's security certificate. At that point, he/she simply clicks on "Continue to this website (not recommended)" to proceed.

To avoid this error message, the WLAN operator can purchase a signed certificate and the RSA private key from an issuing authority. Once these are available, to install them on the switch:

1. Select the *Certificate* configuration tab.
2. Browse to the location of each file. Once located, the name and the path of the RSA private key file and the signed certificate file will appear in the corresponding fields.
3. Click **Upload** to complete the installation.

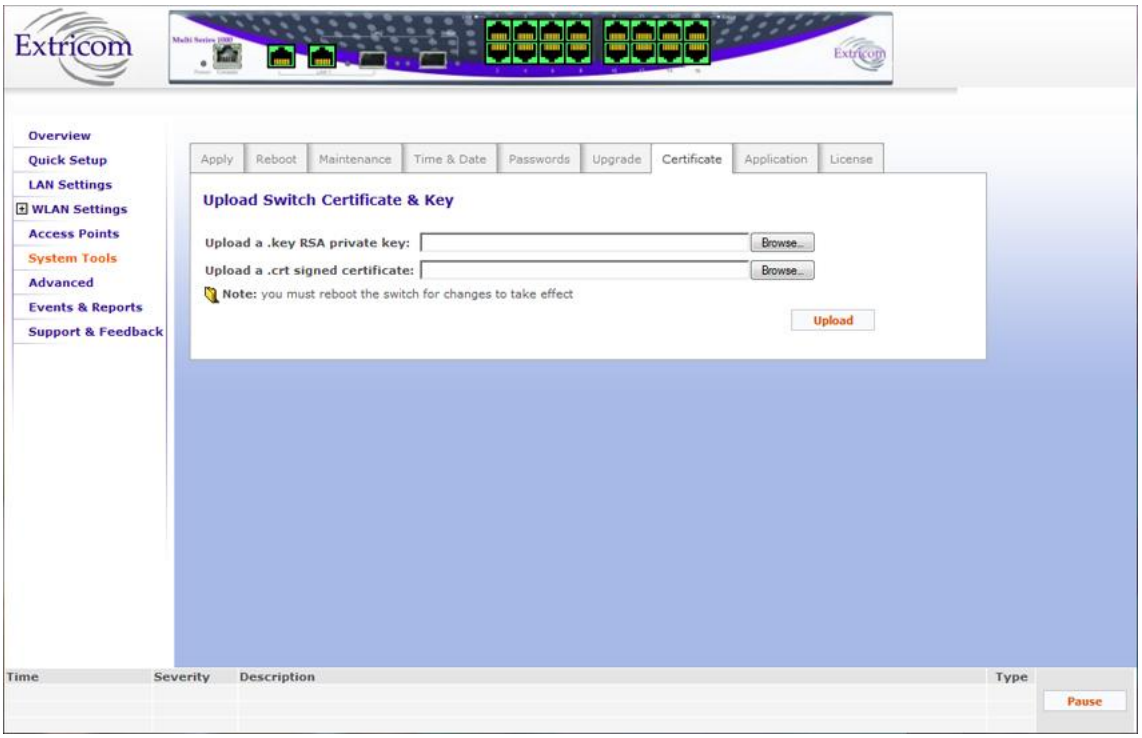


Figure 39: Certificate Configuration Tab

Application

The Application configuration screen is the first one that comes up when configuring a switch cascade (refer to

Installing Switch Cascade section for the details). After the role of each switch is defined, using the Application configuration screen, complete the configuration using the Redundancy configuration screen under the **Advanced** category.

You may also change the role of a switch by accessing the *Application* configuration tab, and selecting one of the Switch Application Types from the drop-down list. The four options are:

- WLAN Switch - refers to a device in standalone mode.
- WLAN Secondary Switch - refers to the backup role of the switch in a switch cascade.
- WLAN Primary Switch - refers to the primary role of the switch in a switch cascade.

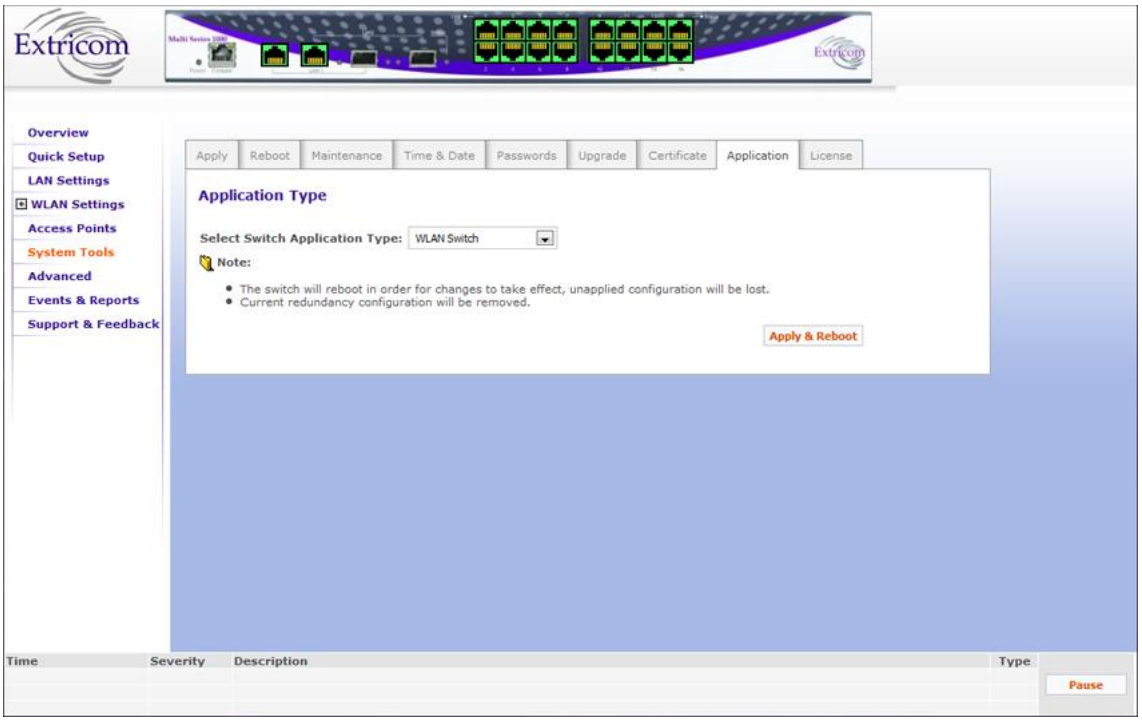


Figure 40: Application Configuration Tab

License

To install the license and activate the switch, click on the License configuration tab.

1. Browse to the location of the License file on your computer.
2. Click **Install & Reboot** to finish activating the switch.

The switch will reboot.

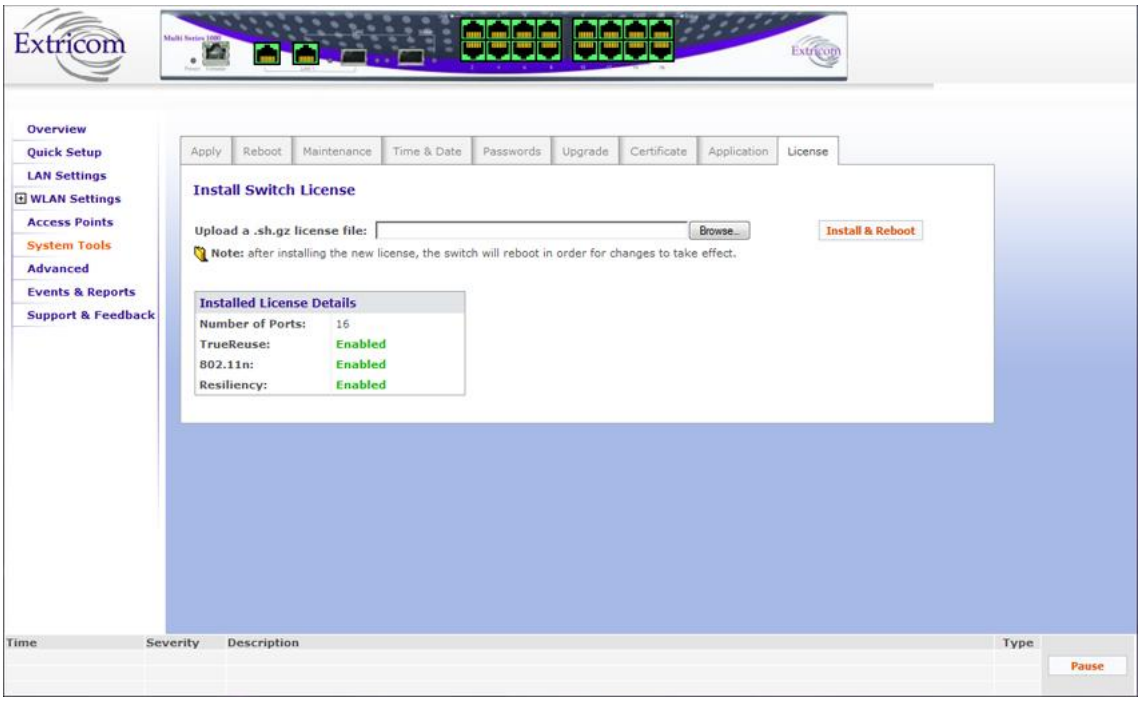


Figure 41: License Configuration Tab

Installing Switch Cascade

1. As described in Chapter 2, connect each switch to a LAN via the LAN1 port, and connect each switch to its APs via WLAN ports.
2. Use LAN2 port for the switch interconnect.
3. Ensure that you have the latest available version of the switch firmware, with Switch Cascade support, on both switches.
4. The secondary switch remains inactive until it is synchronized with the primary switch. When the Primary switch is rebooted, its configuration GUI will be in read-only mode, until the Secondary switch is also rebooted.

Advanced Configuration

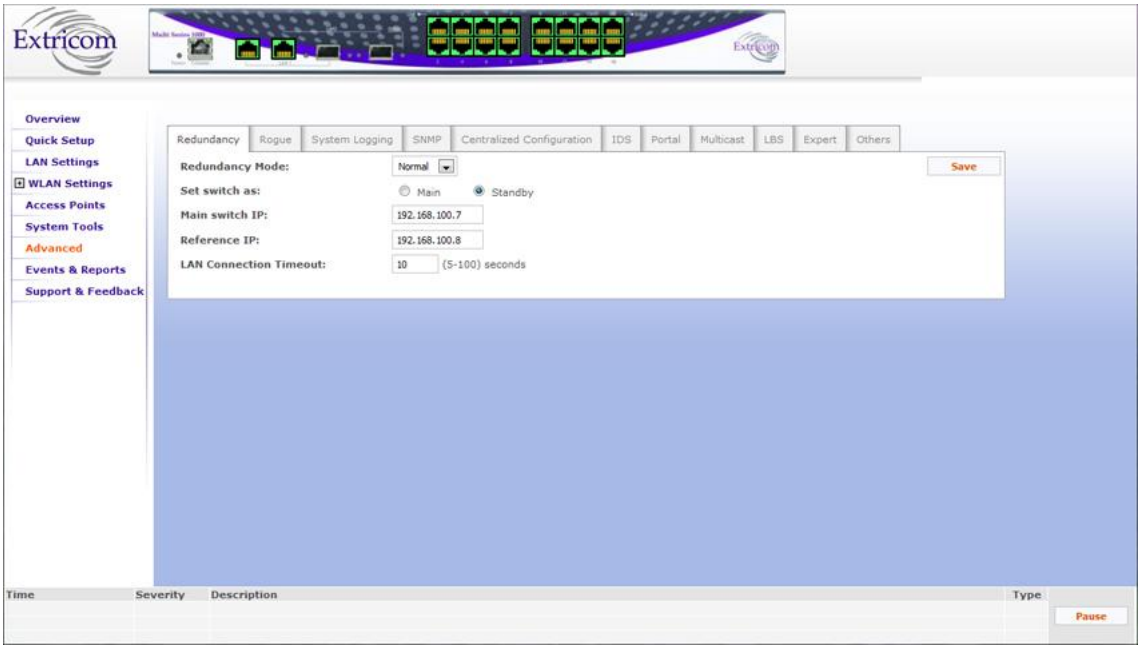
To configure advanced features, select **Advanced** from the navigation tree. Under this configuration category you will find the following configuration tabs:

- Redundancy.
- Rogue.
- System Logging.
- SNMP.
- Centralized Configuration.
- IDS.
- Portal.
- Multicast.
- LBS.
- Expert.
- Others.

Redundancy

1. Switch redundancy refers to redundancy over wired LAN media and provides the master-to-backup auto fallback functionality. Cascade Resiliency supports redundancy between cascaded switches. Both switches are serving a single BSSID until any of them is at fault. As soon as one of the switches fails, the surviving switch serves mobile devices by itself with no human intervention. The eventual replacement of the faulty switch does not necessitate any interruption in service, while returning to a fully redundant mode.

When the Redundancy tab is selected, depending on whether the switch is a part of a cascade or a stand-alone, one of the windows in the Figure 42 below appears:



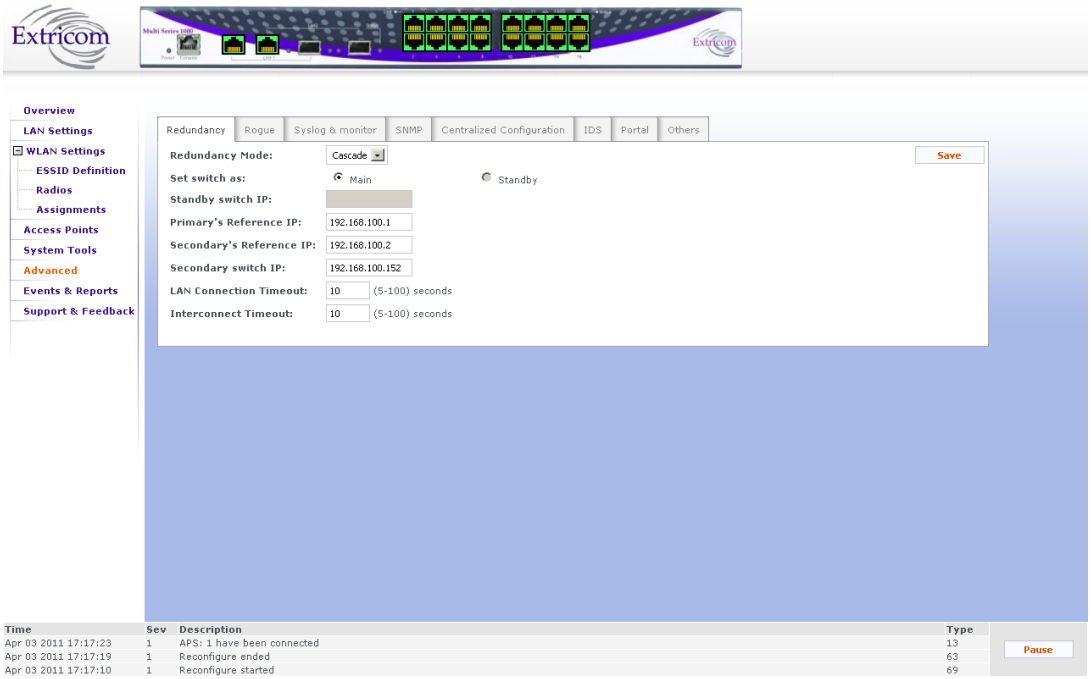


Figure 42: Redundancy Configuration Tab

The fields available *on the Redundancy configuration screen will depend on whether the switch has been set to function as a primary switch in a cascade topology, a secondary one, or it has been set up as a standalone edge switch.*

> **!** To activate a switch cascade, one switch must be set as the Primary, and another switch set as the Secondary, using the Application configuration tab under System Tools. Then, under the Redundancy configuration tab, the Redundancy Mode of the Primary switch must be set to Disable or Cascade. Please refer to the release notes for your firmware version of Switch Cascade.

Redundancy Fields for Primary Switch

The following table lists all available under the *Redundancy* configuration screen fields for a switch that has been set up as a Primary cascade switch. In case of a secondary cascade switch, the same fields will be greyed out.

Field	Description
Redundancy Mode	Select redundancy mode. Possible options are: • **Disable** - no LAN redundancy. A cascaded pair will still provide seamless channel blanket(s) extending across the two switches, but without any LAN redundancy. • Cascade – Switch Cascade with LAN redundancy. • Normal – Legacy mode. Unavailable for cascade switch configuration.
Reference IP	IP address of a reference device on the LAN. This is used to test connectivity to the LAN. The reference device must be operational and respond to pings.
Secondary Switch IP	IP address of the Secondary switch in the cascade pair.
Testing Interval	Interval in Seconds between keep-alive packets sent to the reference IP.

Table 21: Redundancy Configuration Tab Parameters for a Primary Cascade Switch

The Testing Interval and Activate After XX failures parameters monitor LAN link and switch interconnect health.

The Core Redundancy Interval and Core Redundancy Timeout monitor the health of the cascaded switches.

Once the changes are made, you must click Save, then go to System Tools and apply changes as described in the Apply section, in order for them to take effect.

When a switch failure or a link failure has been detected, a failover occurs and the cascaded switch that remains fully operational goes into standalone mode. In two cases below, both switches remain fully operational so they both go into standalone mode. A switch that goes into standalone mode continues to provide switching service to its APs only.

The following table indicates which cascaded APs provide service in the event of a failover, assuming Redundancy mode is set to "Cascade":

Failure Type	Primary APs	Secondary APs	Comments
Switch Interconnect	√	√[1]	Primary and secondary switch failover to standalone mode. Even though APs of both switches are functioning, there is no seamless mobility between the switches.
Primary LAN Link	X	√[1]	Secondary switch failover to standalone mode.

Secondary LAN Link	√	√	No switch failover. Seamless mobility between switches. Secondary switch heartbeat checks of the Primary switch are turned off.
Primary Switch Failure	X	√[1]	Secondary switch failover to standalone mode.
Secondary Switch Failure	√	X	

Table 22: Switch Cascade Failover Behavior

Notes:

1. Traffic interruption time during a failover depends on the link and switch core monitoring parameters chosen (see Table 21 above).
2. √ = Full service
3. X = Not in service
4. The cascaded switches contain the same configuration file, so in the event of a primary or secondary failure, the same configuration file is used by the operational switch.
5. A Primary switch can function as standalone edge switch without requiring a failover.

Once the fault that caused the switchover has been resolved, both switches must be rebooted in order for them to return to normal cascade operation. Otherwise, they will continue to operate in standalone mode.

GUI Operation In Normal Cascade and Failover Operation

The Primary switch GUI is fully operational, if the Primary switch is interconnected to a functional Secondary switch. Otherwise, it is read-only, except for the "Reboot" function and the *Application* configuration tab.

The Secondary switch GUI is always read-only, except for the "Reboot" function and the *Application* configuration tab, regardless of whether the Secondary switch is operating as a secondary switch or as a standalone switch.

AP Overlay Redundancy Mode

In AP Overlay normal redundancy mode, one switch functions as the main switch while the second switch functions in a hot standby mode ("Standby" switch) only. The second switch and all of its APs do not carry any traffic while it is running in hot standby mode. When one of the switchover conditions is met, the standby switch and its APs start carrying traffic. A Normal Redundancy topology is illustrated below:

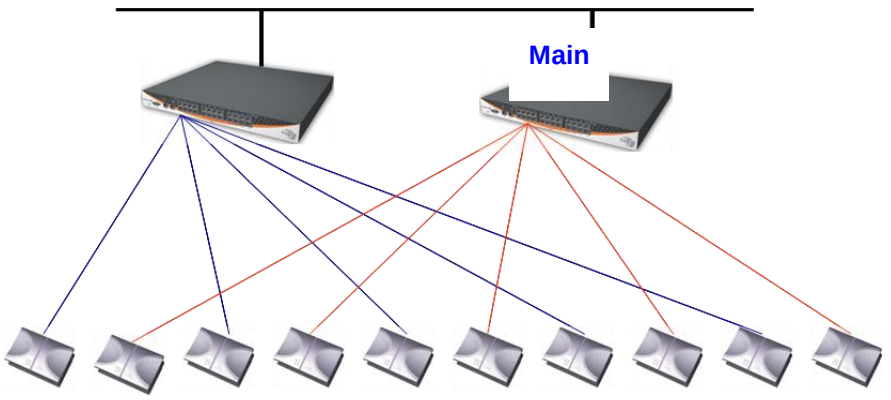


Figure 43: Normal Redundancy Deployment

Redundancy Fields For Standalone Edge Switch

The following table lists all available fields for a standalone edge switch:

Field	Description
Redundancy Mode	Select redundancy mode. Possible options are: • Disable - switch operates as a standalone edge switch. • AP overlay redundancy – switch operates as part of a hot standby configuration.
Set switch as	Designate the switch as a **Main** switch or a **Standby switch.**
Standby switch IP	IP address of the standby switch.
Reference IP	IP address of a reference network element. This is used to test connectivity to the LAN.
Testing Interval	Interval in Seconds between keep-alive packets sent to the reference IP.
Activate After XX failures	The number of lost keep-alive packets before activating failover scenario.

Table 23: Redundancy Configuration Tab Parameters for a Standalone Edge Switch

If “Disable” is chosen in the Redundancy Mode field, all other fields on this configuration page are greyed-out/made inactive.

Rogue

Rogue access points represent the biggest threat to Wi-Fi security. Rogue APs are unauthorized APs that are physically connected to the wired Ethernet LAN.

The Rogue mechanism implemented in the EXSW switches requires a dedicated radio to scan the wireless media and detect Rogue APs. Therefore, one of the radios must be defined as “Rogue” in the Radio Settings page.

The Rogue tab folder allows you to edit a "white list" of independent APs that you allow to operate in your environment.

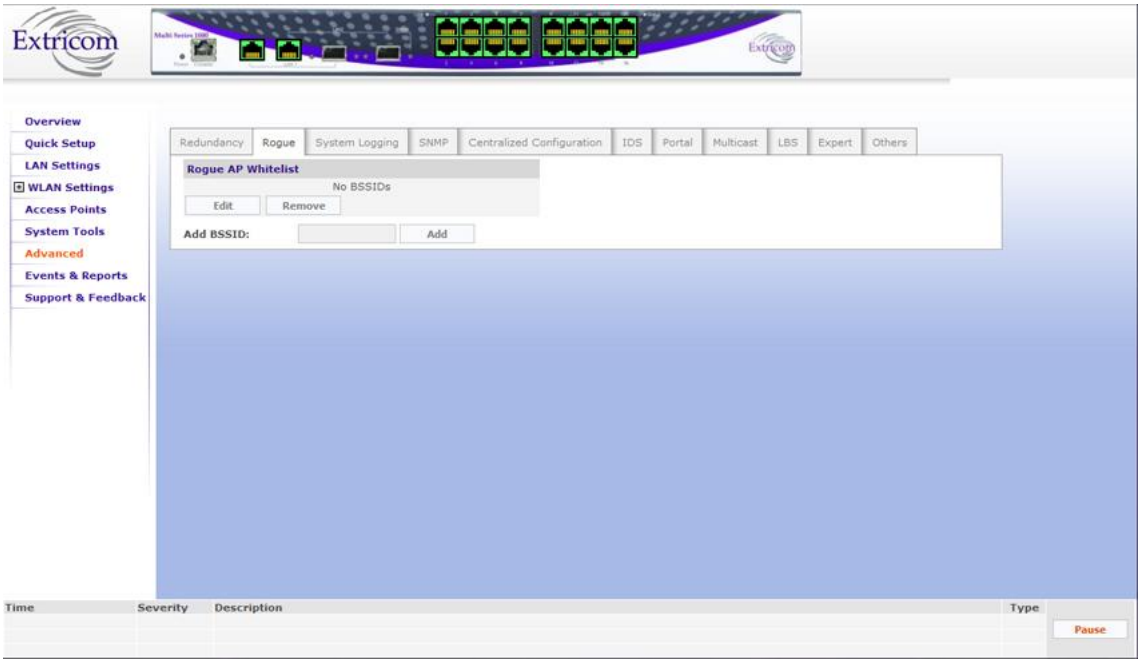


Figure 44: Rogue Configuration Tab

Field	Description
Rogue AP Whitelist	
ADD BSSID	Add a BSSID (MAC address) of an AP that you permit to operate in your network
Edit	Edit the list of legal BSSIDs
Remove	Remove a BSSID from the white list

Table 24: Rogue Configuration Tab Parameters

System Logging

By default the event logging is turned off so as not to overload the LAN. However, you may turn it on using the *System Logging* configuration tab in the Advanced section. To do that:

1. Select the Enable System Logging checkbox.
2. Enter the IP address of the server on which the log will be stored.
3. Click **Save**.

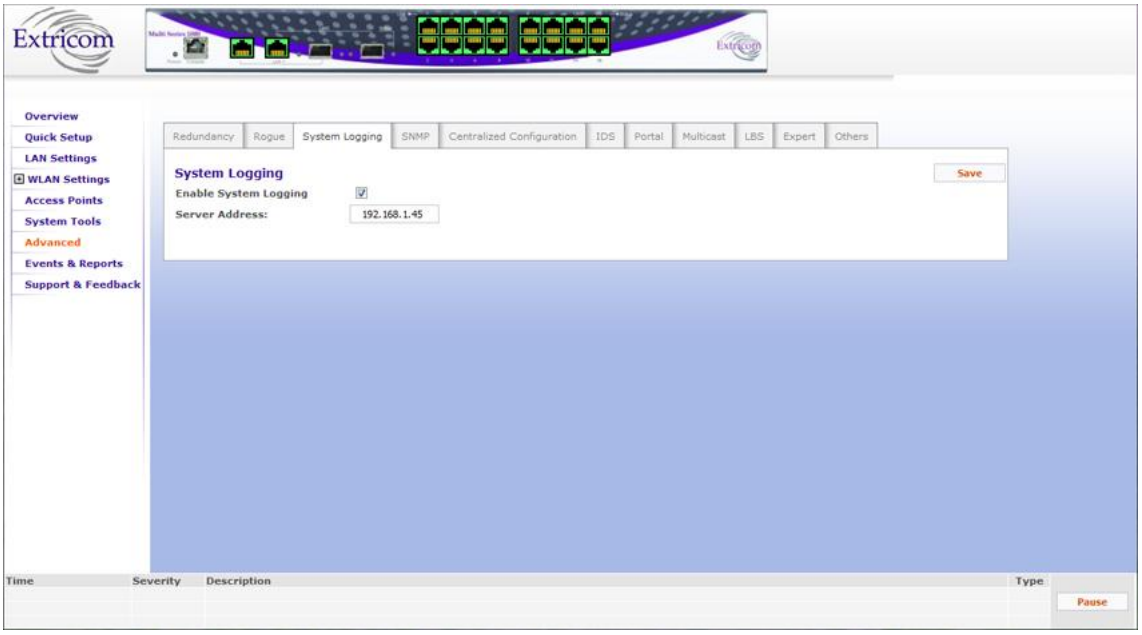


Figure 45: System Logging Configuration Tab

SNMP

Extricom switches generate a wide variety of traps to describe events occurring on the WLAN. In general, these traps can be categorized as follows:

- AP events (connections, disconnections, etc.)
- Client events (associations, disassociations, etc.)
- Switch events
- Configuration events
- Radius events
- Redundancy events (for Switch Cascade)
- Security events (intrusion detection, rogue AP detection, etc.)

Traps are displayed in the Events and Alarms Area at the bottom of the web interface, as illustrated in the Figure 46 below.

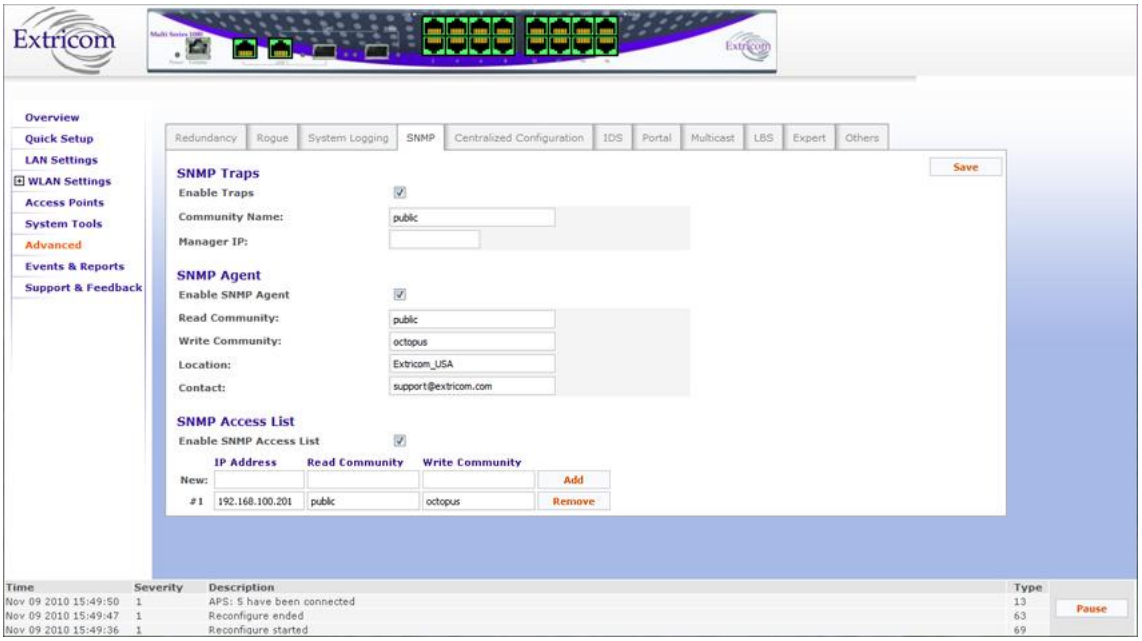


Figure 46: SNMP Configuration Tab

SNMP Traps

Traps can also be sent by the switch over its northbound interface to network management devices, such as Extricom's EXNM-2000. To begin sending SNMP traps over the northbound interface, configure the **SNMP Traps** section under the *SNMP* tab as follows:

1. Select the **Enable Traps** checkbox.
2. Enter a desired name in the **Community Name** field.

3. Enter the IP address of the manager device in the **Manager IP** field.

Please see Chapter 5 (Northbound SNMP Traps) for a complete list of SNMP traps that may be sent by an Extricom switch.

SNMP Agent

You may configure the switch to respond to SNMP queries from various management systems on the network. To do that:

1. Enable the function by selecting the **Enable SNMP Agent** checkbox.
2. Set the password for SNMP Get-Requests by entering it in the **Read Community** field.
3. Set the password for SNMP Set-Requests by entering it in the **Write Community** field.
4. Enter the location of the switch in the **Location** field.
5. Enter the contact information in the **Contact** field.

SNMP Access List

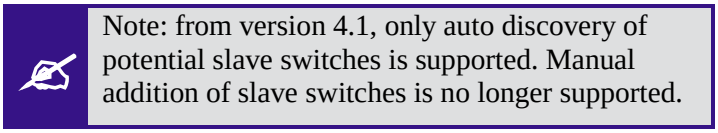
To tighten security of your wireless LAN you may decide to configure specific access lists (ACLs) to grant SNMP access to specific devices. To do that:

1. Enable the SNMP ACL function by selecting the **Enable SNMP Access List** checkbox.
2. Enter the IP address of a device, along with the Get-Request and Set-Request passwords in the **Read Community** and **Write Community** fields respectively.
3. Click **Add**.

Enter as many ACL as needed. Before navigating away from this configuration screen, do not forget to save the changes you made by clicking Save button on the right. To start generating SNMP traps, you must apply configuration.

Centralized Configuration

Centralized Configuration allows you to manage a group of identical Extricom switches (*slaves*) from one single *master* switch. You must decide which switch will act as a *master*. Extricom switches have a built-in mechanism to discover the presence of other Extricom switches.


Note: from version 4.1, only auto discovery of potential slave switches is supported. Manual addition of slave switches is no longer supported.

Configuration changes on the *master* switch are propagated to the *slave* switches via a secured mechanism. For this authentication scheme to work, the *slave switches* need to obtain a copy of the *master*'s public key prior to the centralized configuration. This is done in the initial phase of the switch's configuration by first retrieving the *master*'s public key and then uploading it to the designated *slave switches*.

Initial Setup

1. Configure the LAN settings on the *Master* switch.
2. Generate an SSH key pair on the *Master* switch. This is done by first designating the switch as a master by clicking in the **Enable Master** checkbox, then clicking the **Generate** button (see Figure 47 below).
3. Save the generated SSH Key file on your PC.
4. Manually configure the LAN settings for each of the *Slave* switches as described in the Configuring LAN Parameters section of this manual.
5. Upload generated by the *Master* switch SSH key file onto every *Slave* switch you wish to manage from this specific *Master*. This is done by clicking the **Browse** button and navigating to the previously saved SSH key file, then clicking **Save**, once the file name appears in the **Set key from disk** field (see below).

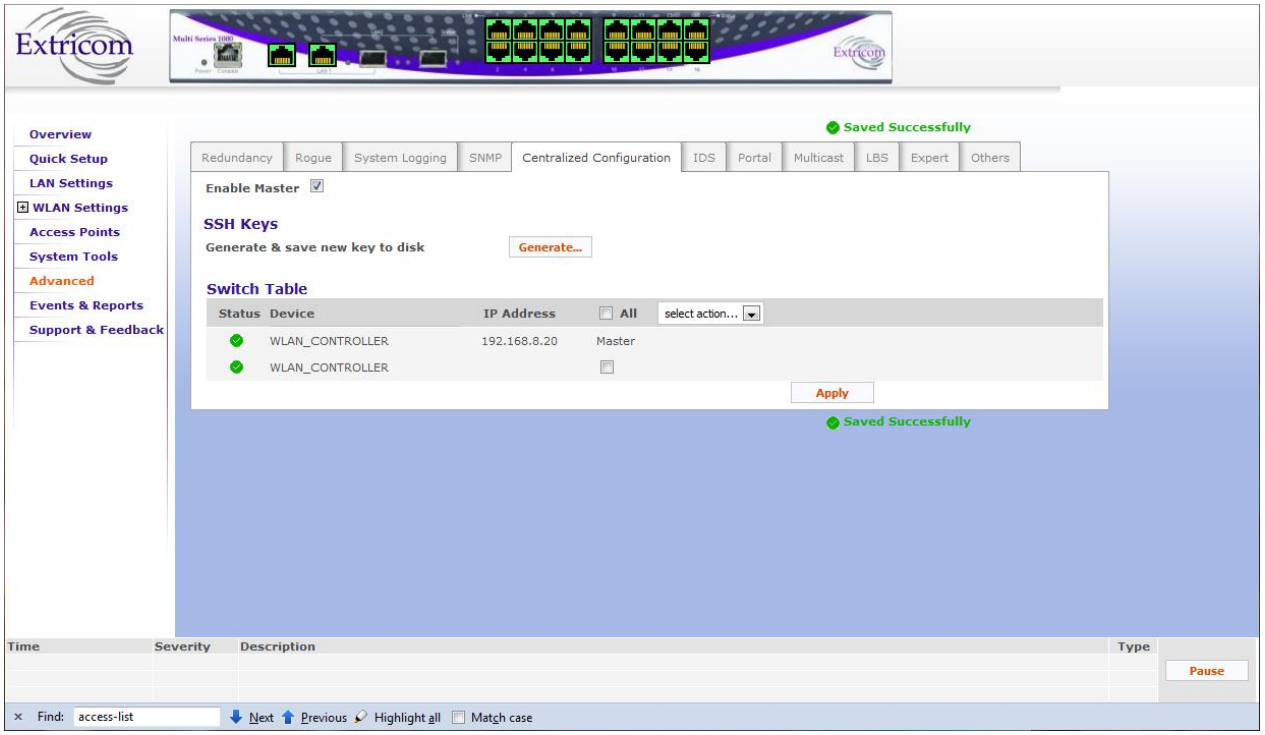


Figure 47: Centralized Configuration Tab for Master Switch

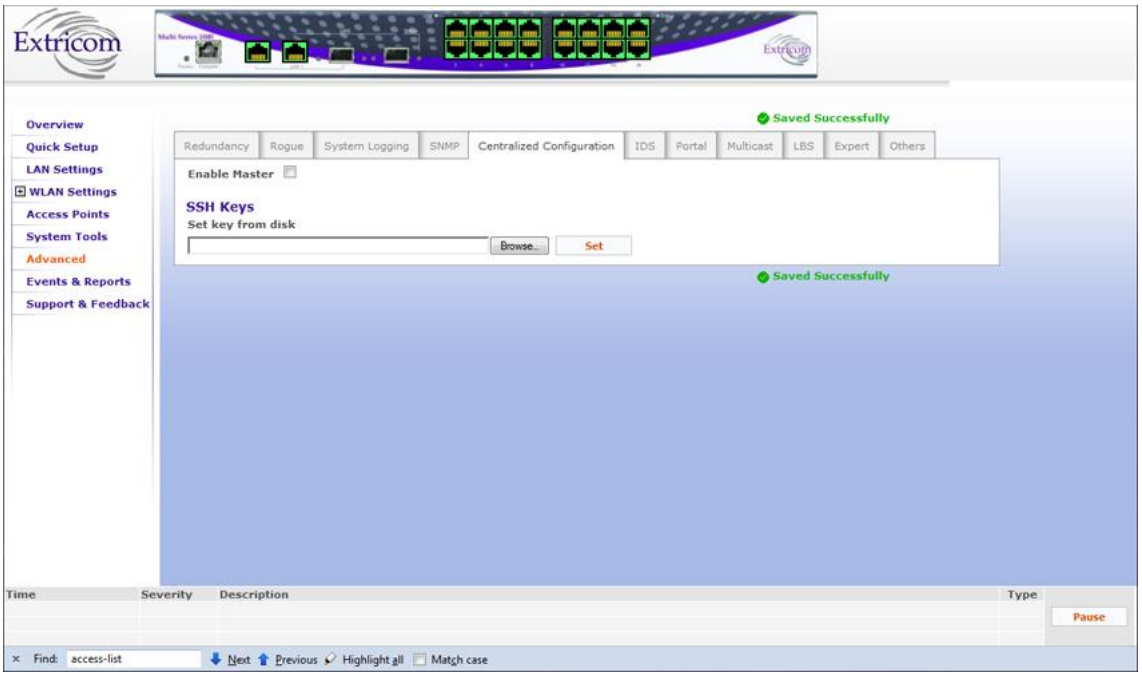


Figure 48: Centralized Configuration Tab for Slave Switch

Slave Switch Configuration

1. On the *Master* switch, open the *Centralized Configuration* web page and in the **Switches Table** section select all the slave devices that you wish to update by clicking on the corresponding checkboxes.
2. Select **reconfigure** from the drop down menu on the right, then click **Apply**. The configuration will be loaded onto each selected *Slave* switch.
3. To reboot slave switches from the master, mark corresponding checkboxes, select the **reboot** option from the drop-down menu, and click **Apply**.

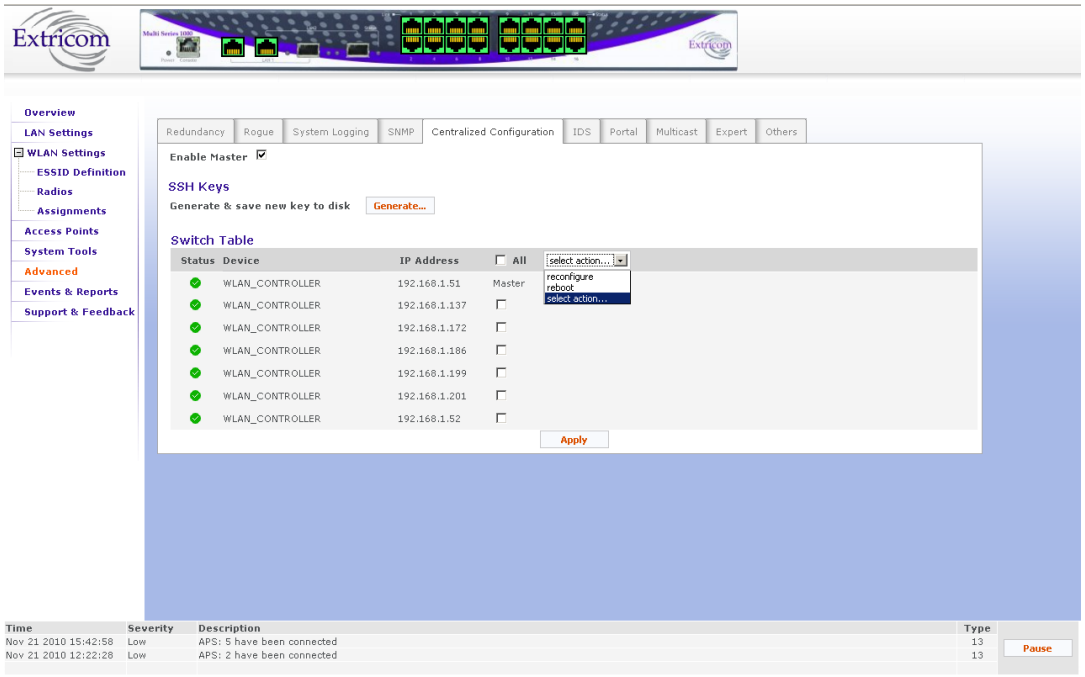


Figure 49: Slave Control Action Options On Master

IDS

Malicious WLAN clients can cause a “denial of service” condition by flooding the WLAN network. A denial of service condition is identified through attack signatures or other factors, most of which are well-known. The IDS tab allows the user to enable this mechanism, set thresholds for identifying an attack and choose types of attacks to be detected. The IDS mechanism detects 802.11 duration attacks and 802.11 management message flooding attacks. Upon attack detection, the system sends a Trap message notifying of the event, and when applicable, provides the attacker’s details (i.e. MAC address). Network administrators can use this information to take action and block malicious users. To configure IDS services refer to the Table 25 below for the specific parameters.

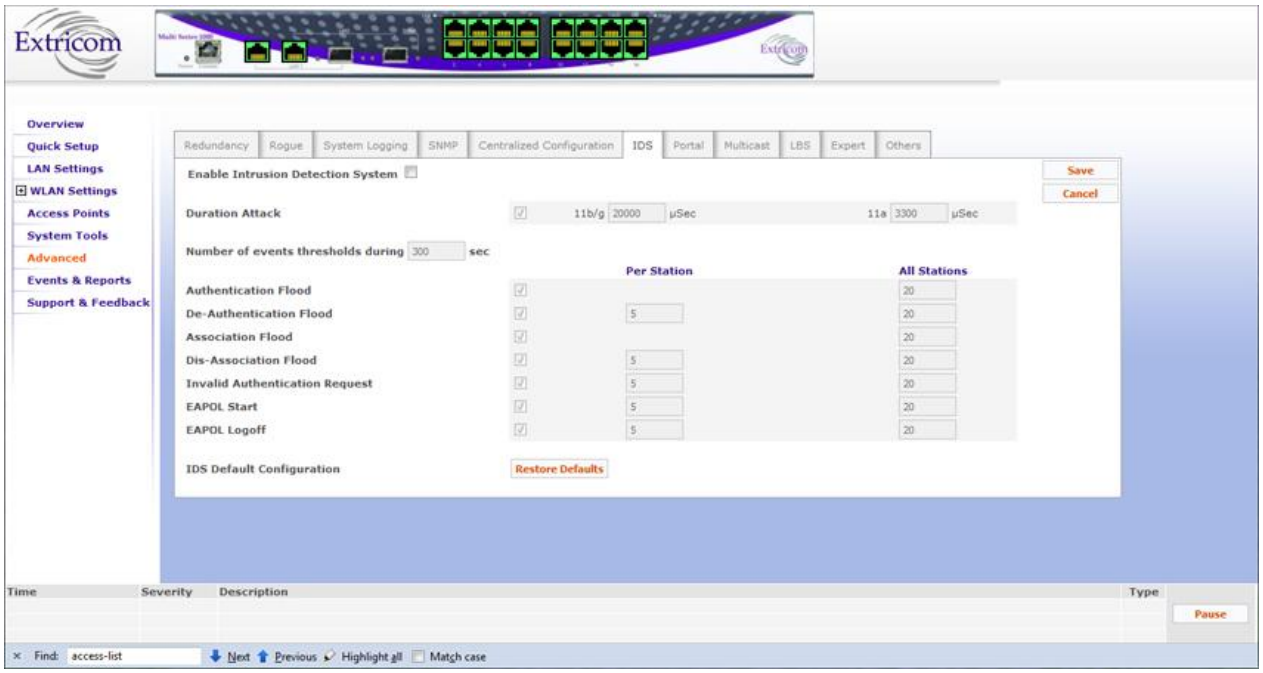


Figure 50: IDS Configuration Tab

Field	Description
Enable	Enables Intrusion detection
Duration Attack	
	WLAN devices reserve the channel for a particular period of time and then start using the radio channel. This time period is the Network Allocation Vector (NAV) in 802.11. .By using high NAV values, an attacker can prevent other WLAN devices from utilizing the wireless network.
Enable	Select check box to enable this feature.
11b/g , 11a box	Define the Max NAV period (in µsec), after which attack is detected.
Flood attacks	
	Malicious users can flood the WLAN with 802.11 management messages
Number of Events Thresholds During xx Sec.	Time window (in seconds)

Field	Description
Per station	Number of times a specific event is allowed during the event threshold. Each of the possible attack types listed below is assigned a limit **per station**
All station	Number of times a specific event is allowed during the event threshold. Each of the possible attack types listed below is assigned with a limit to **all stations**
Authentication Flood	Flooding the WLAN with authentication requests
De-Authentication Flood	Flooding the WLAN with de-authentication requests
Association Flood	Flooding the WLAN with association requests
Dis-Association Flood	Flooding the WLAN with dis-association requests
Invalid Authentication Request	Flooding the WLAN with invalid authentication requests
EAPOL Start	Flooding the WLAN with EAP authentication ”EAPOL Start”
EAPOL Logoff	Flooding the WLAN with EAP authentication ”EAPOL Logoff”
Defaults	
Restore defaults	IDS Default Configuration

Table 25: IDS Configuration Parameters

Portal (Captive Portal)

The Captive Portal mechanism restricts user Internet access by redirecting user web access requests to a Captive Portal web page.

There are two Captive Portal web page types:

- **SSL-based Secured Logging**: In Secured Logging, a user is initially authenticated before he/she is allowed internet access. The user enters the username and the password using SSL. The Switch then authenticates the user via RADIUS Server. Secured Logging is used for applications that require authentication-based access such as hotels, guest access, etc.
- **Open Access**: In an Open Access model, a user trying to access the web is redirected to a welcome web page, which might, for example, contain Terms of Use to which the user must agree before being allowed internet access. Open Access is used for applications that enable open access such as free Airport networks, etc.

The *Portal* tab allows you to configure the following Captive Portal settings:

- Enable/Disable Captive Portal.
- Set Captive Portal parameters.
- Set Pre-Authentication Allowed Destinations (Walled Garden) parameters.
- Define Additional Networks.
- Define a Customized Default Page.
- Upload your own Customized Page.

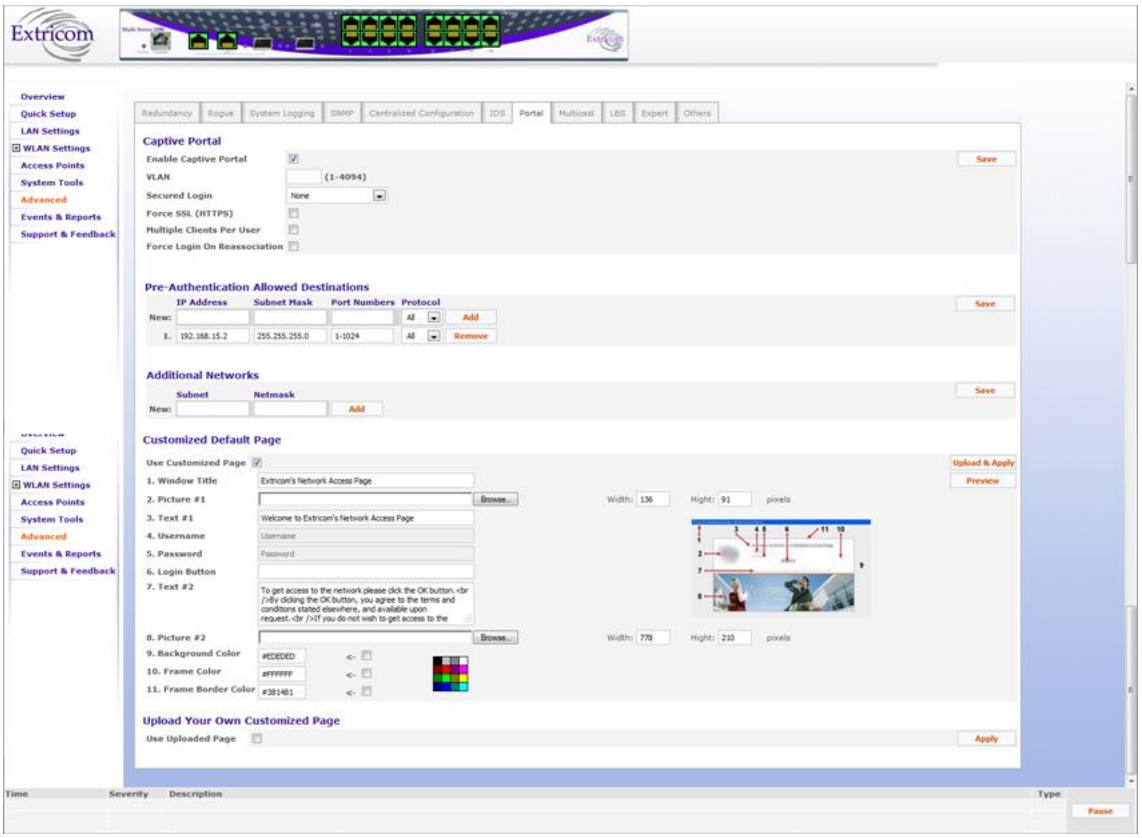


Figure 51: Captive Portal Configuration Tab

To configure Captive Portal, refer to the table below:

Field	Description
Enable captive portal	You must enable this option system-wide if you want to configure captive portal on any ESSID.
VLAN	Set the Captive Portal VLAN. When ESSID is set to be Captive Portal restricted, the ESSID VLAN is automatically set to this VLAN
Secured Login	Set the type of Authentication - either Local, or Remote (Radius). When selecting Remote Authentication, select a Radius server, and Authentication Protocol (PAP or CHAP)
Force SSL (HTTPS)	When this option is selected, any client that attempts to connect using http: will be redirected to SSL (https:) communication. If this feature is not activated, the type of session will depend solely on the protocol (http:// or https://) specified at the beginning of the URL string entered into the client's browser.
Multiple Clients Per User	Enables multiple simultaneous client connections with the same user name and password via the portal.

Field	Description
Force Login on Re-association	Configure log-in without authentication on re-association.
Pre-Authentication Allowed Destination (Walled Garden)	You can define a list of up to 10 free access network destinations (10 rules). WLAN clients associated to the captive portal restricted ESSID can reach these destinations without going through the Captive portal authentication process. A network destination (a rule) is defined by an IP address, Subnet mask, Port Numbers and an Internet Protocol (TCP, UDP, ICMP).
Additional Networks	You may add trusted networks by specifying a Subnet along with its Netmask for each such network.
Customize Default Page	If you don't check the "Use Customized Page" check box , then the captive portal web page will be set to Extricom default web page, otherwise follow the instructions to customize the page.
Upload Your Own Customized Page	Allows you to upload your own captive portal web page. Use the **instruction** link to build your web page.

Table 26: **Captive Portal Configuration Parameters**

Figure 52: Extricom Default Captive Portal Web Page

Multicast

Under the *Multicast* configuration tab you may limit the amount of time the system is busy with sending Multicast traffic.

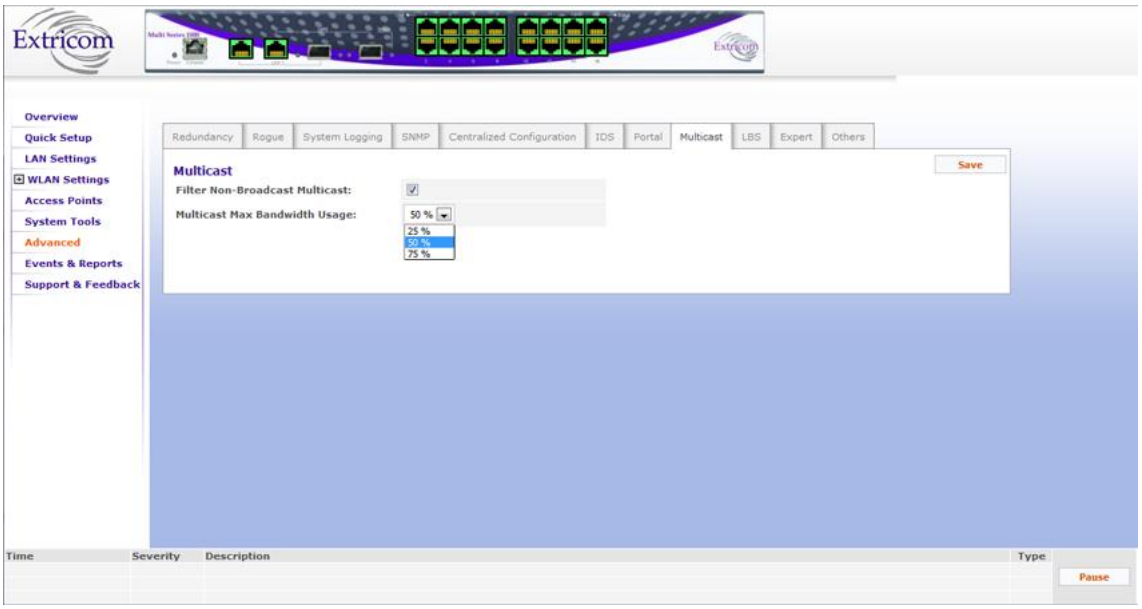


Figure 53: Multicast Configuration Tab

LBS

1. Location-Based Service (LBS) tab: **Real Time Location Services (RTLS)** support 3rd party RTLS solution vendors which provides high accuracy location based services for WLAN mobile clients.

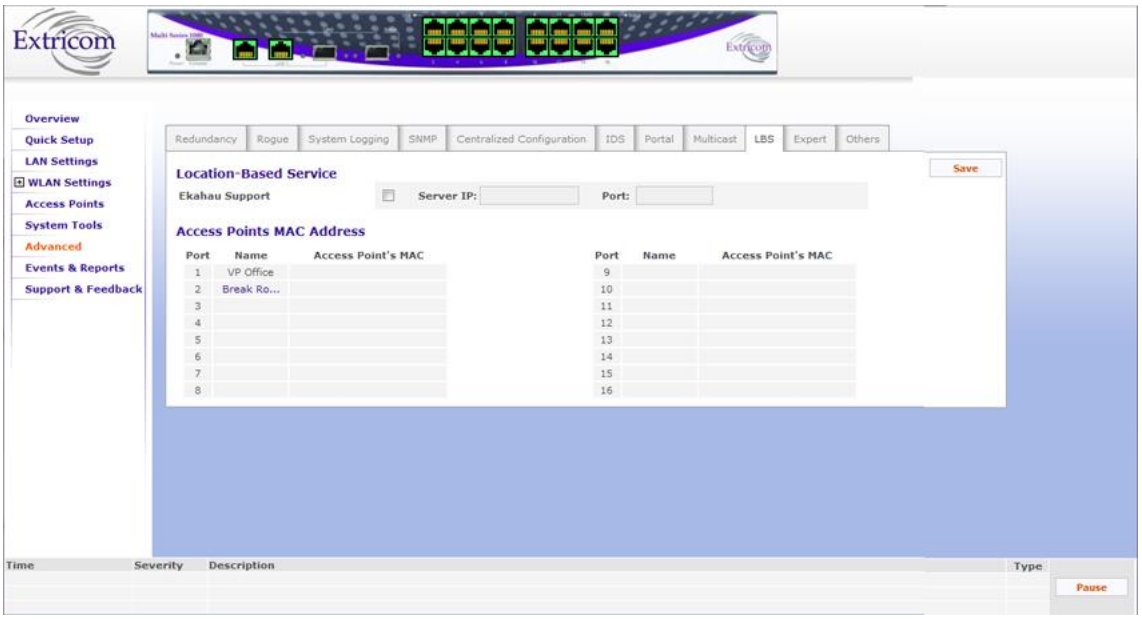


Figure 54: LBS Configuration Tab

Expert

Here you may activate the **Expert User Mode** by selecting the checkbox and clicking **Apply**.

Figure 55: Expert Configuration Tab

Others

Under the *Others* tab, a number of advanced configuration options, such as 802.11d, are provided.

- Select the **802.11d Support** checkbox if you wish to enable this option. You can enable it per ESSID or for all ESSIDs.
- Select the **MAC Authentication** checkbox if you wish to enable this option.
- Select the **Beacon Rate Control** checkbox if you wish to enable this option.
- Select the **WMM** check box if you wish to enable this option .You can enable it per ESSID or for all ESSIDs.
- Select the **Beacon Rate Control** check box if you wish to enable this option.
- Select the **In Band Management** checkbox if you wish to enable this option (This is a general enabling of the option and requires per ESSID configuration).
- Select **Band Steering** checkbox if you wish to enable this option.

To activate these options per ESSID, after selecting the above checkboxes refer to the Configuring WLAN Settings section of this guide.

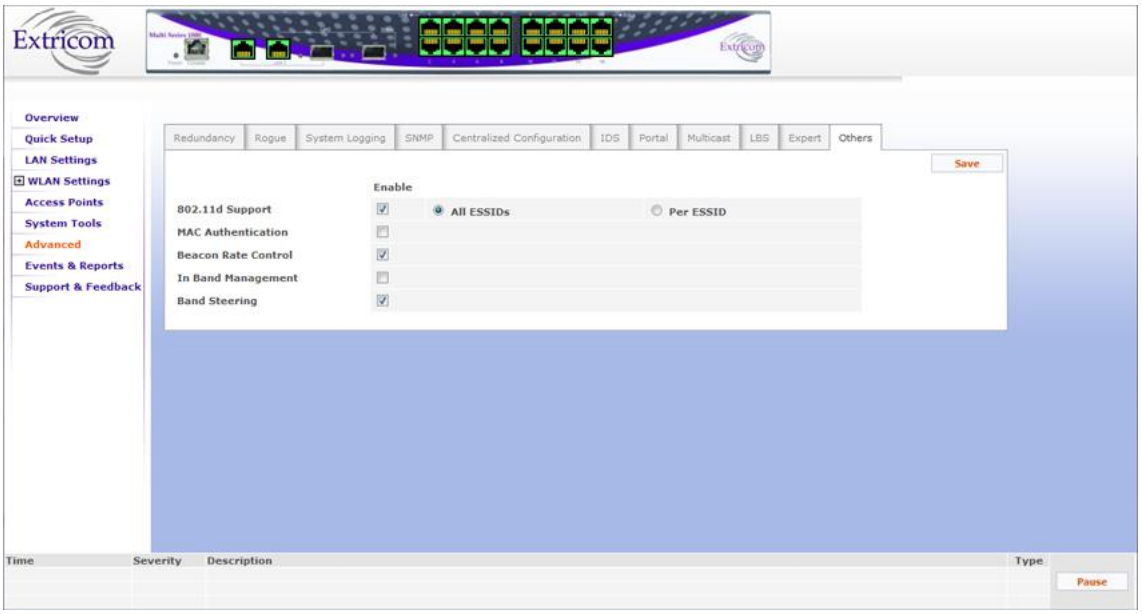


Figure 56: Others Configuration Tab

Viewing Events and Reports

The *Events & Reports* page provides performance reports and lists various system events. To access this page click **Events & Reports** in the navigation tree. Within the page you will find the following configuration tabs:

- System Events
- Clients Events
- Events Filter
- Reports
- Diagnostics

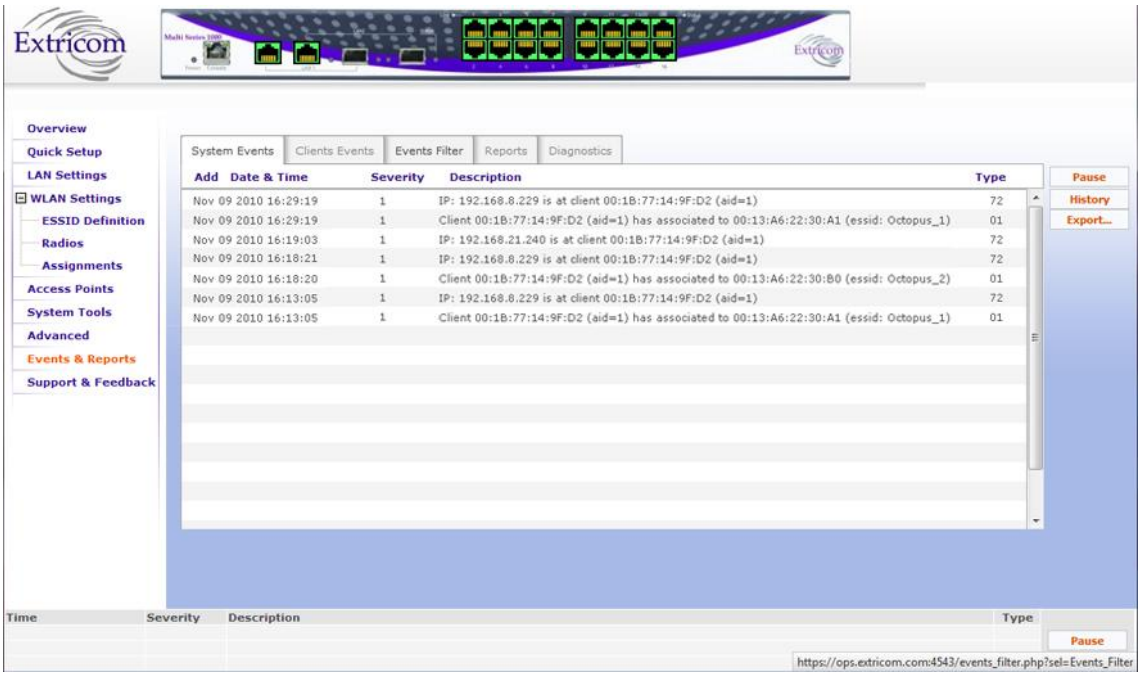

Extricom
Overview
Quick Setup
LAN Settings
WLAN Settings
ESSID Definition
Radios
Assignments
Access Points
System Tools
Advanced
Events & Reports
Support & Feedback
System Events
Clients Events
Events Filter
Reports
Diagnostics
Add Date & Time Severity Description Type
Nov 09 2010 16:29:19 1 IP: 192.168.8.229 is at client 00:1B:77:14:9F:D2 (aid=1) 72
Nov 09 2010 16:29:19 1 Client 00:1B:77:14:9F:D2 (aid=1) has associated to 00:13:A6:22:30:A1 (essid: Octopus_1) 01
Nov 09 2010 16:19:03 1 IP: 192.168.21.240 is at client 00:1B:77:14:9F:D2 (aid=1) 72
Nov 09 2010 16:18:21 1 IP: 192.168.8.229 is at client 00:1B:77:14:9F:D2 (aid=1) 72
Nov 09 2010 16:18:20 1 Client 00:1B:77:14:9F:D2 (aid=1) has associated to 00:13:A6:22:30:B0 (essid: Octopus_2) 01
Nov 09 2010 16:13:05 1 IP: 192.168.8.229 is at client 00:1B:77:14:9F:D2 (aid=1) 72
Nov 09 2010 16:13:05 1 Client 00:1B:77:14:9F:D2 (aid=1) has associated to 00:13:A6:22:30:A1 (essid: Octopus_1) 01
Pause
History
Export...
Time Severity Description Type
Pause
https://ops.extricom.com:4543/events_filter.php?sel=Events_Filter

Figure 57: Events & Reports - System Events Tab

System Events

The *System Events* tab lists system messages that where generated by the switch as event notifications. Date & Time of occurrence, as well as the Severity of the event are also displayed.

Clients Events

The *Clients Events* tab lets you view client association and disassociation events only. Just like in the case with the System Events, each client event is displayed with corresponding Date & Time of its occurrence and level of Severity.

On both System Events page and Clients Events page there are three buttons on the right side of the screen: **Pause/Continue** toggle, which lets you stop or start the flow of the events; **History**, which brings up the list of the most recent past events (up to 1000); and **Export**, which lets you save an event log into a .CSV file on your computer.

If a message is signed with a sign in the **Add** field, by clicking on this message, the MAC address of the associated with the message user will be automatically inserted into the MAC ACL list.

Events Filter

You may exclude some of the events from your reports, using the *Events Filter* configuration tab. Select the checkbox(es) corresponding to those events, and click **Save**.

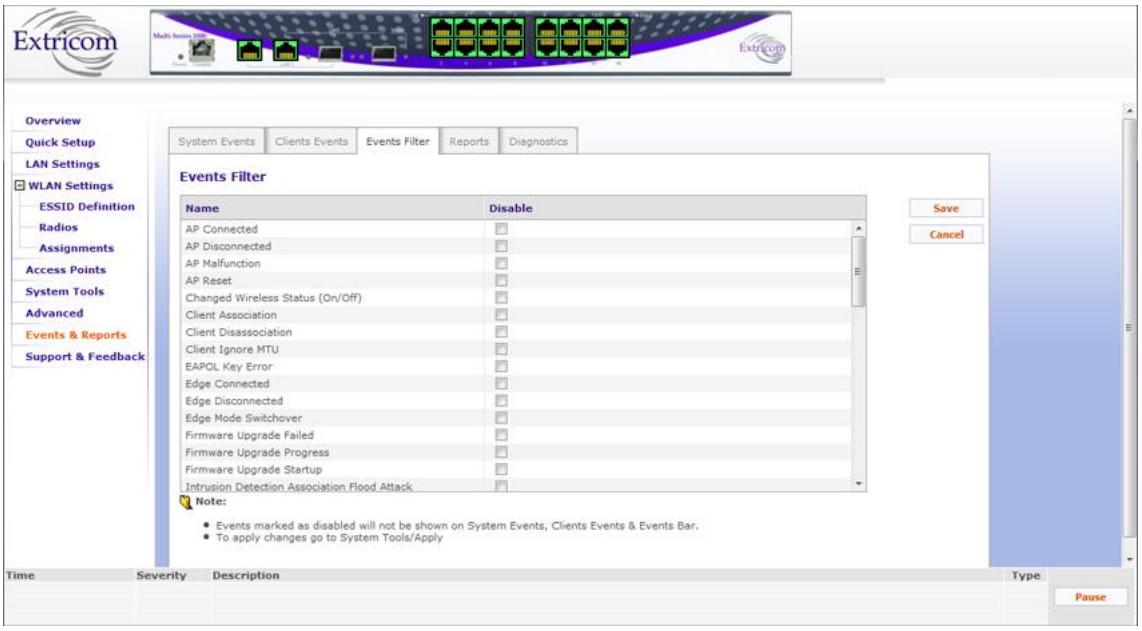


Figure 58: Events Filter Configuration Tab

Here is the list of the events reported by default:

- AP Connected
- AP Malfunction
- AP Off
- AP Reset
- Changed Wireless Status (On/Off)
- Client Association
- Client Disassociation
- Client Ignore MTU
- EAPOL Key Error
- Edge Connected
- Edge Disconnected
- Edge Mode Switchover
- Firmware Upgrade Failed
- Firmware Upgrade Progress
- Firmware Upgrade Startup
- Intrusion Detection Association Flood Attack
- Intrusion Detection Authentication Failure Attack
- Intrusion Detection Authentication Flood Attack
- Intrusion Detection De-Authentication Broadcast
- Intrusion Detection De-Authentication Flood Attack
- Intrusion Detection Disassociation Flood Attack
- Intrusion Detection Duration Attack

- Intrusion Detection EAPOL Logoff Attack
- Intrusion Detection EAPOL Start Attack
- Intrusion Detection RF Jamming Attack
- Last Radius Failed
- License Failed
- POE reset
- RF Localization Failed
- Radio Is Functioning Normally In All Access Points.
- Radio Is Not Functioning In Access Points
- Radio Malfunction
- Radio Reset
- Radius Changed Selection
- Radius Timeout
- Reconfigure Ended
- Reconfigure Started
- Redundancy Keepalive Connection Down
- Redundancy Keepalive Connection Up
- Redundancy Peer Connection Down
- Redundancy Peer Connection Up
- Redundancy Status Down
- Redundancy Status Up
- Rogue AP Found
- Rogue AP Lost
- Rogue AP Update
- Set Client IP
- Start.sh Ended
- Start.sh Started
- Starting Boot

Reports

The Reports window, shown below, provides a wide range of per radio channel based and per switch based statistics.

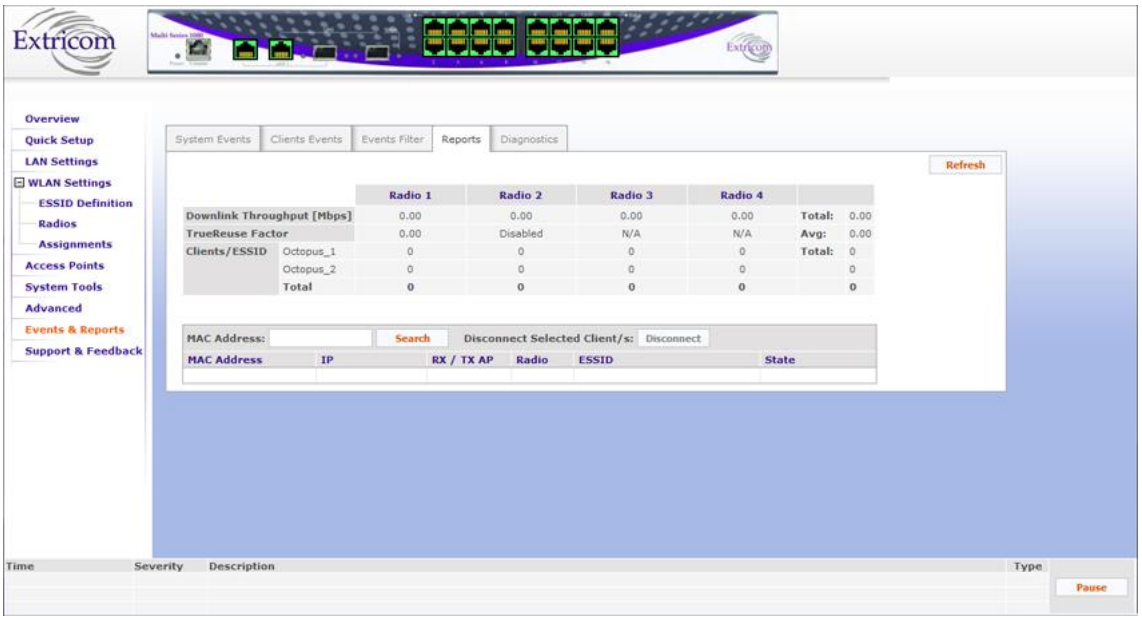


Figure 59: Reports Tab

The following table describes the information available on this page:

Field	Description
Downlink Throughput [Mbps]	A one-second long snapshot of the data volume carried by all downlinks on a particular radio channel (channel blanket).
Total	Total downlink throughput of the switch, based on a 1 second snapshot of data volume.
TrueReuse Factor	Available only if TrueReuse is enabled. Ranges from 1-3. Indicates the current downlink throughput relative to what the downlink throughput would have been if TrueReuse was not enabled. Computes the average number of downlinks transmitting simultaneously per radio channel. The average is computed based on several snapshots taken during several1 second time intervals. Example: a value of 3 means that downlink throughput with TrueReuse is currently 3x higher on average on that radio channel than if TrueReuse had been disabled.
Avg.	TrueReuse Factor average over all radio channels.
Clients /ESSID	Number of clients connected per ESSID per radio channel.
Clients/ESSID Total	Total number of clients per ESSID per radio channel, over all channels, per switch.

Field	Description
MAC Address	Used to search for a MAC address on the page. Any matching MAC address in the list of clients' MAC Addresses will be highlighted.
Disconnect Selected Client/s	Used to reset a client connection, in order to help a client establish a working connection. The client must then re-authenticate to reconnect to the WLAN.

Table 27: Reports Window Fields

Note: the statistics window does not get updated automatically. Click **Refresh** to update the statistics.

At the bottom of the screen in this tab folder, the clients (MACs) per AP are listed, along with the information on MAC/IP/RX-TX AP/Channel/ESSID/State.

Diagnostics

In this section you may collect various media usage, traffic, network health, and other relevant statistics, as well as initiate various real-time tests. The area for data requests and test initiating is located in the left section of the configuration screen. The results are displayed in the right portion of the screen, and may also be downloaded to your computer. Refer to the Table 28 below for the details on diagnostics parameters and types of tests available.

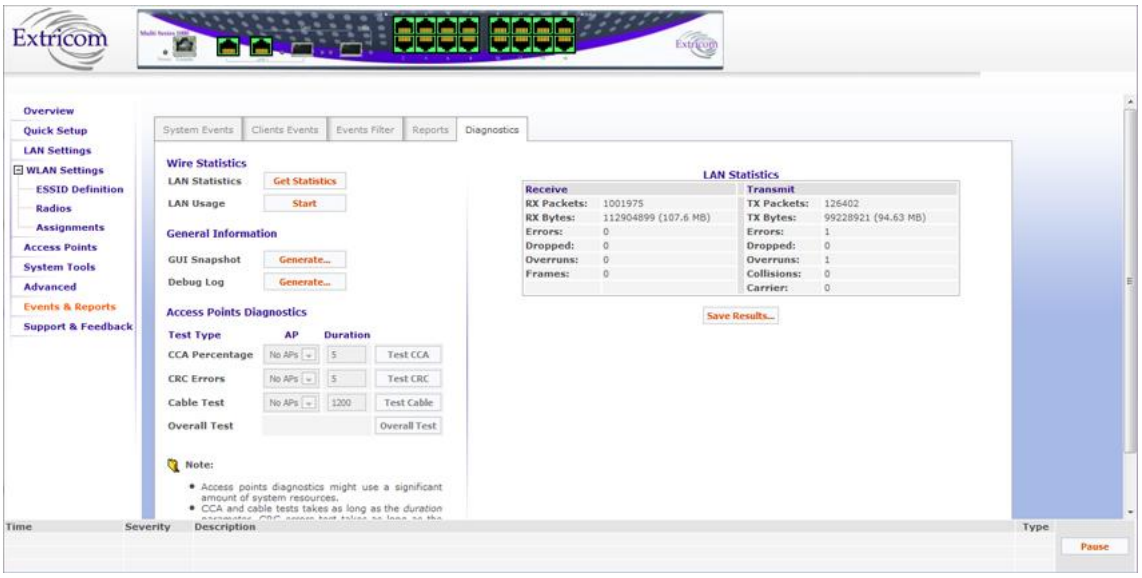


Figure 60: Diagnostics Tab

Field	Description
Wire Statistics	
LAN Statistics	Click **Get Statistics** to get information about the transmit (TX) and receive (RX) traffic on the LAN, in Packets and in Bytes. Here you also receive information on errors, drops, overruns, etc. Clicking **Save Results** below the table in the right portion of the screen exports those results into an .html file.
LAN Usage	Click **Start** to begin collecting the LAN data on receive (RX/Downlink) and transmit (TX/Uplink) traffic in real time (in Mbps). To terminate data gathering click **Stop**.
General Information	
GUI Snapshot	Clicking **Generate** begins generating a series of statistics snapshot which are organized into a series of files and packaged into a compressed archive of .html files.
Debug Log	Click **Generate** to dump a log into a .log file.
Access Points Diagnostics	
CCA Percentage	Clear Channel Assignment result in 0-100% percentage. A higher value indicates there's more medium consumption. Duration is measured in Seconds. This function impacts the WLAN service. Select an AP from the drop-down list, specify duration of the test in seconds, and click **Test CCA**.

Field	Description
CRC Errors	CRC (cyclic redundancy check) errors indicate the number of frames received with errors (accidental changes to raw data). Select an AP from the drop-down list, specify duration of the test in seconds, and click **Test CRC**. CRC errors test takes as long as the duration parameter multiplied by the number of radios.
Cable Test	Initiates a data transfer to measure drop packets threshold. Recommended duration for cable test is 1200 seconds.
Overall Test	Initiates all three tests - CCA Percentage, CRC Errors, and Cable Test. The results are displayed in the right portion of the screen.

***Table 28:* Diagnostics Tab Parameters and Tests**

Overview of the Configuration

1. The *Overview* page provides a summary of the current configuration. To get to it, click **Overview** in the navigation tree.

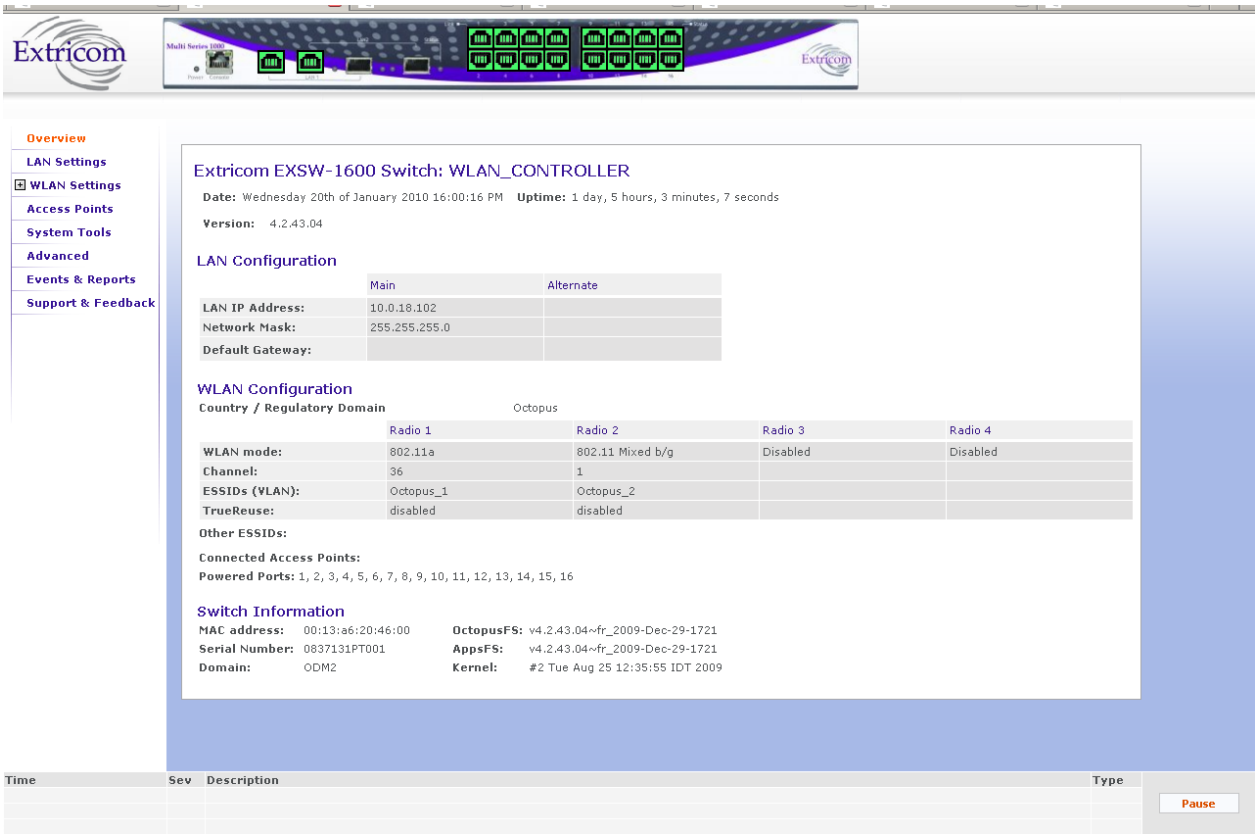


Figure 61: Configuration Overview of MS-1000

Field	Description
Date	Displays the date and time the summary was created.
Uptime	Displays the amount of time the switch has been up since the last reboot.
LAN Configuration	
Main	IP address of the switch.
	Network mask.
	The IP address of the default gateway.
WLAN Configuration	
Country/Regulatory Domain	Displays the regulatory domain name currently in use by the switch.
WLAN mode	Displays the WLAN mode for each radio. (Disabled, 802.11a, 802.11b, 802.11g, 802.11b/g, 802.11n/a, 802.11n/g, 802.11n/b/g, or Rogue)
Channel	Displays the channel for each radio.
ESSIDs (VLAN)	Displays the ESSIDs and their related VLANs, defined and assigned to each radio.
TrueReuse	Shows whether TrueReuse is enabled or disabled for each radio.
Other ESSIDs	Displays other ESSIDs that are defined but are not assigned to any specific radio.
Access Points & PoE Configuration	
Connected Access Points	List of the active APs.
Powered Ports	List of WLAN ports which have PoE enabled.
Switch Information	
MAC address	Displays the base MAC address of the switch.
Serial Number	Displays a unique serial number of the switch.
Domain	RF localization indication.
OctopusFS:	Extricom firmware application version and build date.
AppsFS	Third-party software application version and build date
Kernel	Extricom-specific Linux kernel build date

Table 29: **Summary of the Overview Page**

Chapter 4

Configuring the Extricom LS-3000 System

The Extricom LS-3000 Solution

The Extricom LS-3000 Switch

The Extricom LS-3000 switch typically drives up to eight edge switches and attaches to the network via one or two IEEE802.3ad link aggregation ports. Mobiles are associated directly with the LS-3000. Network configuration details such as security profile, SSIDs, assigned channels to blankets, and VLAN assignments, are maintained in the Extricom LS-3000.

The Extricom Edge Switch

Each Edge switch (an Extricom MS-1000 switch) drives up to sixteen access points with power, and connects the APs to the infrastructure through the Extricom LS-3000. Mobile devices are not managed by the edge switch.

Access Points

Extricom access points have up to three radio modules each operating on a different channel, and providing up to 450 Mbps. The access points are driven by one IEEE802.3z PHY and supports 802.3af Power over Ethernet. Power may be delivered by either the edge switch or the Extricom range extender on the copper port.

Media Converter (Optional)

The media converter is a device used to convert between copper Ethernet and Fiber Ethernet when required. This extends the reach of the Extricom LS-3000 to the edge switch beyond the 100m limitation of IEEE 802.11.3z. The total length supported between the Extricom LS-3000 and the access point is about 700 meters. The total length of copper Ethernet is 100 meters.

Extricom Network Management System (NMS)

The Extricom NMS is a management system designed to control and log single and multiple Extricom LS-3000 deployments from a single network entity. The NMS comprises a server and one or more client devices. The NMS is provided on read only media with license scaling according to the number of AP ports required.

Redundancy

The Extricom LS-3000 software supports warm failover between two overlying Extricom LS-3000 full deployments. As long as System A is functioning correctly, System B remains in standby mode. If a fault is detected in System A, System B commences service on a different BSSID. Once System A returns to proper functionality, it becomes the backup system.

Unpacking the Extricom LS-3000 System

The Extricom WLAN LS-3000 system is shipped with the following:

- One Extricom LS-3000 switch.
- MS 1000 (EDGE) switches (the number of EDGE switches is based on the customer order and provided in separate boxes) are shipped as part of the overall order.
- CD which contains license serial number.
- APs (the number of APs is based on customer order and provided in separate boxes) are shipped as part of the overall order.
- One power cable for the LS-3000 switch and one for each of the EDGE switches.
- Mounting brackets with screws.

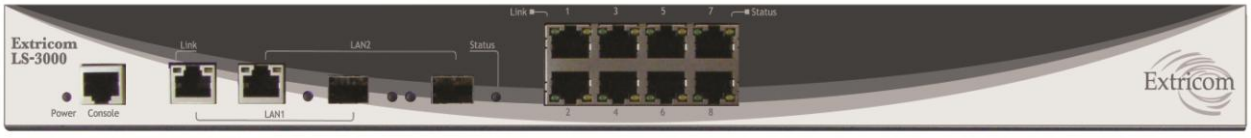


Figure 62: Extricom Large LS–3000

Connecting the LS-3000 Switch

To connect a switch to the EDGE switches and access points:

6. Using a CAT-5e/6 100/1000Mbps cable, connect the RJ-45 LAN1 connector located on the front panel of the switch (refer to Figure 62) to the LAN switch.
7. Using a CAT 5e/6 100/1000Mbps cable, connect the RJ-45 LAN1 connector located on the front panel of each EDGE switch to one of the LS3000 switch's RJ-45 WLAN connectors.
8. Using a CAT-5e/6 cable, connect each AP (refer to Figure 12 and Figure 16) to one of the EDGE switch's RJ-45 WLAN connectors.

> AP distances of up to an additional 700m can be supported on GbE connections by using Extricom EXMC-1000 media converters. For more information, refer to EXMC-1000 Media Converter

9. Connect the power cable to the power connector located on the rear panel of the LS-3000 switch, and plug the other end of the power cable into a power source.

10. Connect the power cables to the power connectors located on the rear panel of the EDGE switches, and plug the other end of the power cables into a power source.

11. Verify that the Power LEDs on all the switches and connected APs are green.

	Additional APs can be connected /disconnected while the switch is active.

	If using fiber media converters (ATI/100Mbps, CTC/1000Mbps) to extend switch-to-AP distance: • Each converter requires external power. • Once all cables are connected (Switch – copper – converter – fiber – converter – copper – AP) perform a port power down/up in the web GUI of the switch to renew switch awareness of the AP connection. • Fiber mode is Multi for 100Mbps. • Fiber mode can be Multi or Single for 1000Mbps per the SFP module selected. Note both ends of the fiber termination must be in the same (SFP) mode.

Accessing the Extricom LS-3000 Switch GUI

After connecting the switches and APs, configure the Extricom WLAN system through Extricom's web configuration GUI using a terminal or PC connected to the same LAN as the switch.

To access the Extricom web-based configuration tool:

1. In your Web browser, enter the following: **`https://<IP address of the switch>`** where **`<IP address of the switch>`** is the IP address of the switch provided with your purchase. Note that **https** must be used, *not* http, in order to initiate a secure browsing session (SSL) with the switch.

	Prior to opening the configuration tool, make sure your console PC is configured with an IP address in the same subnet as the switch.
	If you did not receive a switch IP address with the switch, the factory default value for the switch IP address is 192.168.1.254.
	If you are using the default IP settings, do not place a router between the user PC and the switch.

2. On the first login you will receive a notice in your browser that there is a problem with the website's security certificate. Click "**Continue to this website (not recommended)**".

3. The *Login* page appears, as shown in Figure 18:

4. Enter the user name and password of the system integrator and click **OK**. The *Summary* page appears.

If you did not receive a user name and password with your switch, use the following factory default user name and password:

user name: *admin*
password: *Switch1*

The user name and password are case-sensitive.

If you use Internet Explorer 8 web browser to configure the switch, you will receive a notice in a pop-up window stating that there is a problem with the website's security certificate.

Press the **Tab** key on your keyboard until you see the link **Continue to this website (not recommended)**, and click on it.

Using the Extricom Web Configuration Pages

The Extricom Web Configuration pages have four main areas:

- Switch image – The Extricom Web configuration page displays an image of the configured switch (the MS-500, or the MS-1000) at the top of the page; the image shows dynamic status of the PoE of each AP port (grey = PoE off, green = PoE on).
- Navigation tree
- Configuration display, and editable work area (for some screens)
- Event and alarm area

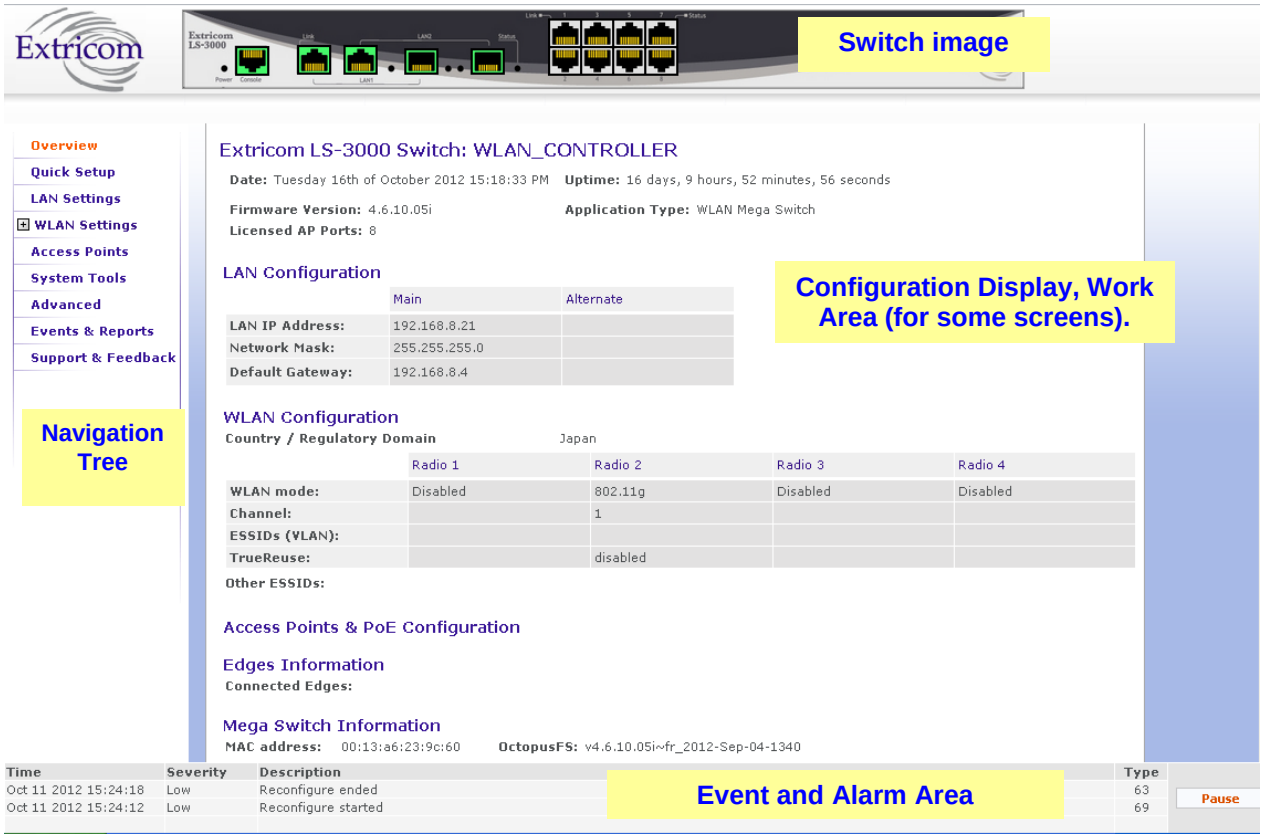


Figure 63: Typical Web Configuration Page

For more information on this page, refer to **Error! Reference source not found.** on page **Error! Bookmark not defined.**

If you do not select **Apply** (in the **System Tools** configuration section) after clicking **Save**, the new configuration will only take effect after the switch is rebooted.

If you change the IP address of the switch, and the new IP address is on the same subnet as the previous one, you will not lose the connection session. If, however, the new IP address is on a subnet, different from the one your PC is on, the connection session will be lost. In this case, you will have to configure your PC with a new IP address that is in the same subnet with the switch and start a new https session

Using the Quick Setup Wizard

The Quick Setup Wizard is a tool designed to guide users through the necessary steps required for a basic LS-3000 configuration. Once the switch is configured using the Quick Setup Wizard, the settings can be fine-tuned and adjusted according to the needs of the system.

> IMPORTANT! Using the Quick Setup Wizard will overwrite any existing LAN and WLAN settings. You may wish to save your current configuration data to the disk. For more information, refer to Maintenance on page 65.

To initialize the Quick Setup Wizard:

1. Select Quick Setup from the Navigation Tree. The following screen appears.

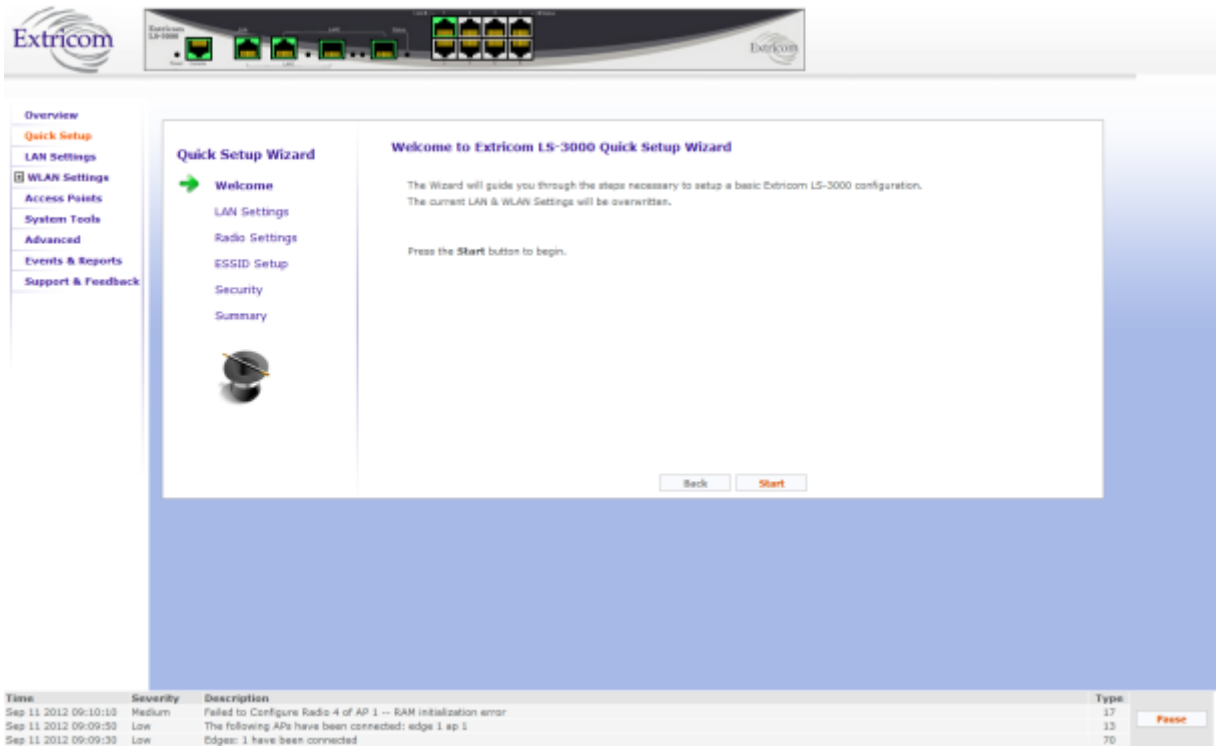


Figure 64: Quick Setup Wizard

2. Click **Start**. The **LAN Settings** configuration window appears.

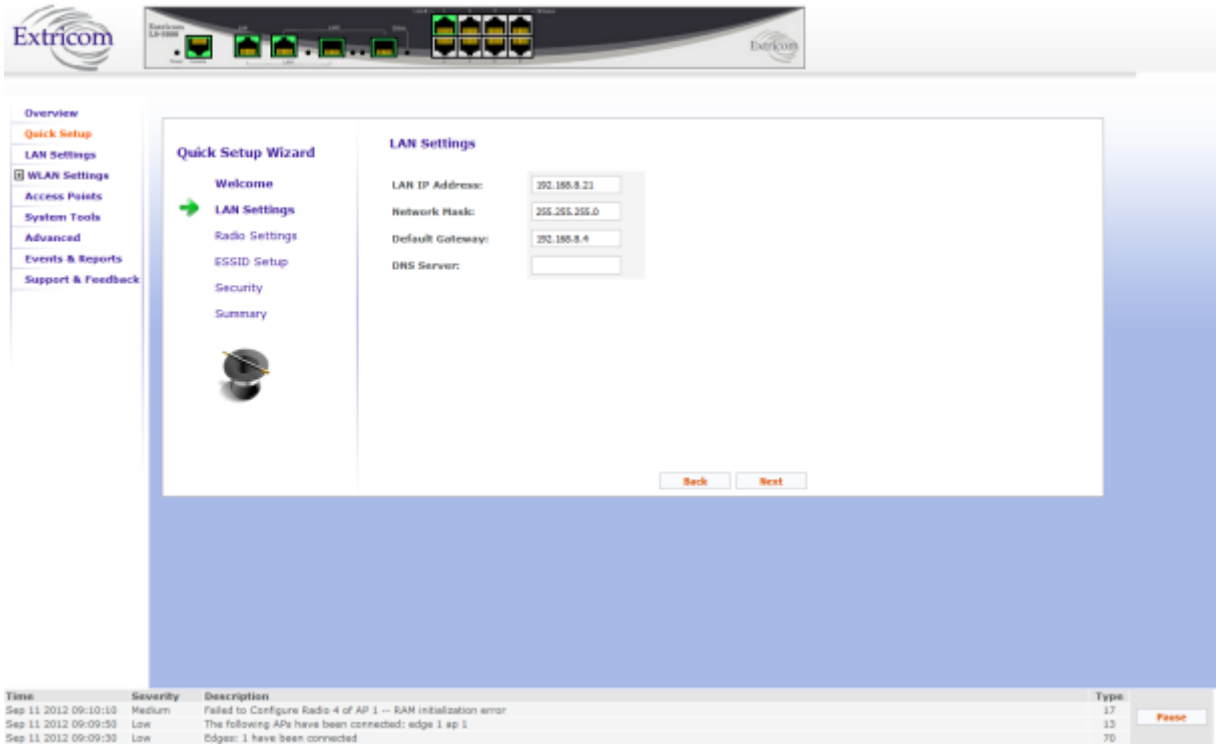


Figure 65: LAN Settings Configuration window

3. Enter the following information:
   - **LAN IP Address**
   - **Network Mask**
   - **Default Gateway**
   - **DNS Server**
4. Click **Next**. The **Radio Settings** window appears.

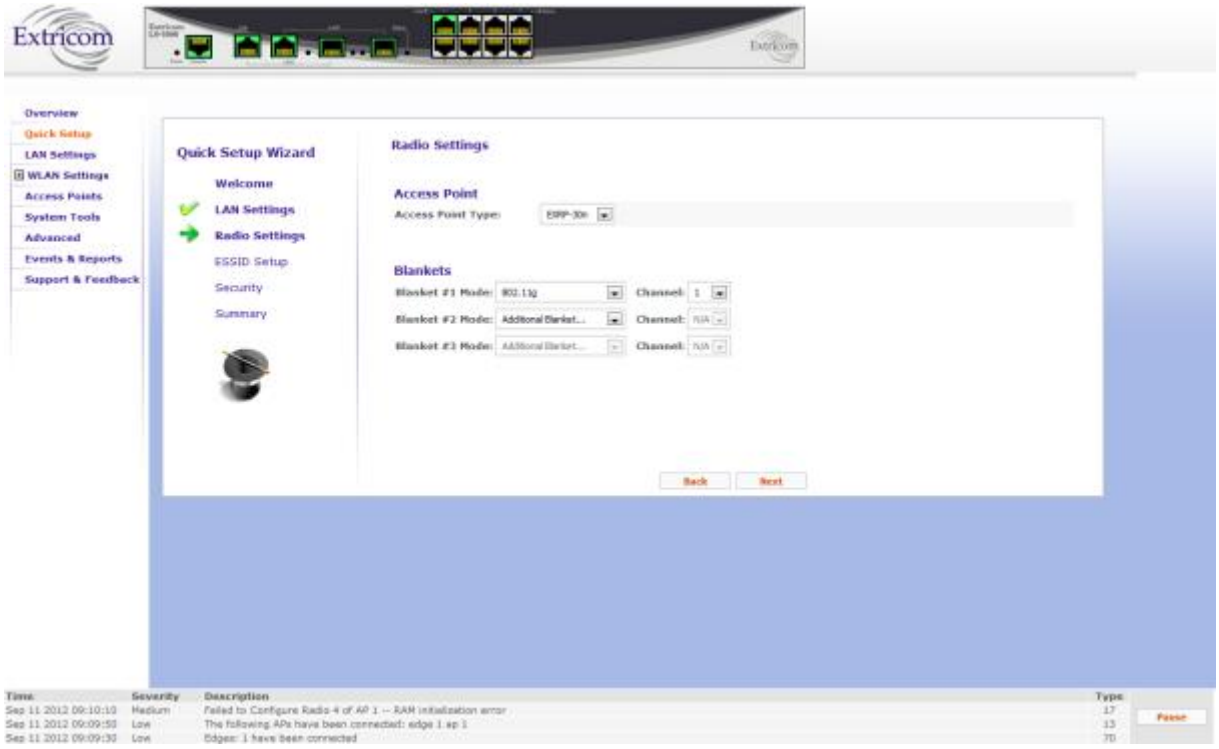


Figure 66: The Radio Settings window

5. Select the Access Point type, and configure the blanket modes and channels.
6. Click **Next**. The **ESSID Settings** window appears.

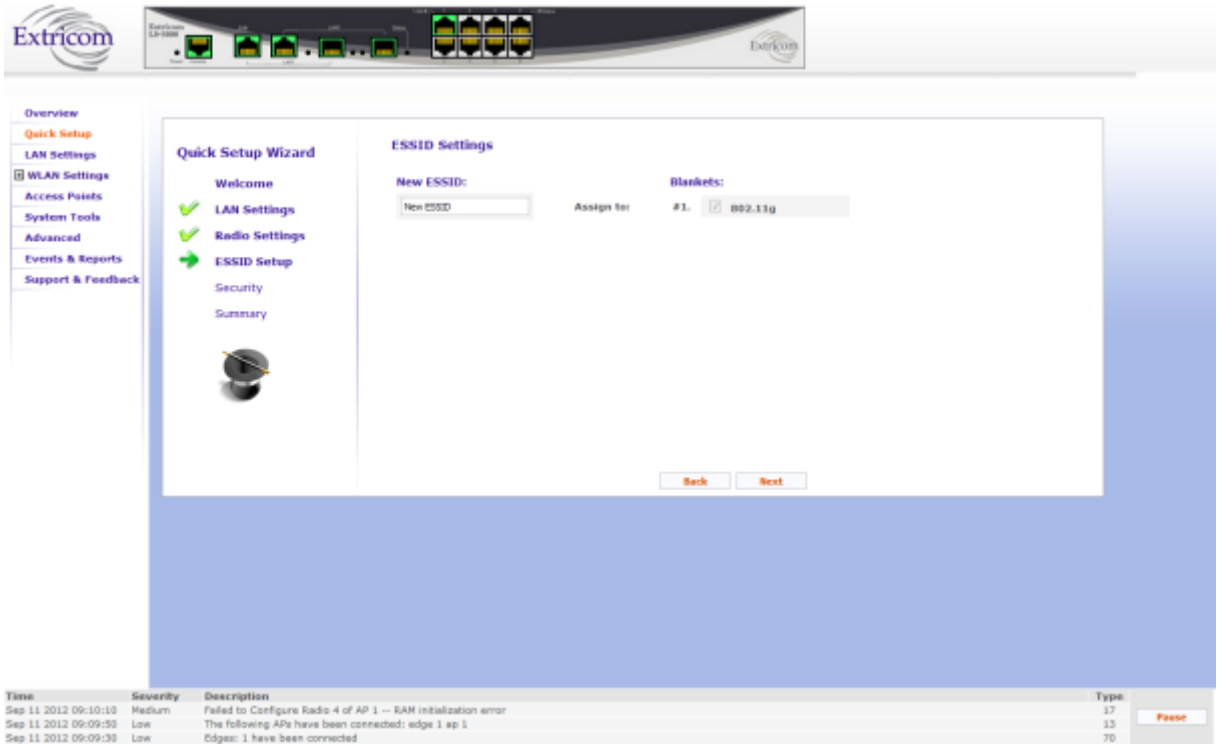


Figure 67: The ESSID Settings window

7. Enter the name of the new ESSID and select to which Blanket to assign it.
8. Click **Next**. The **SSID Security** window opens.

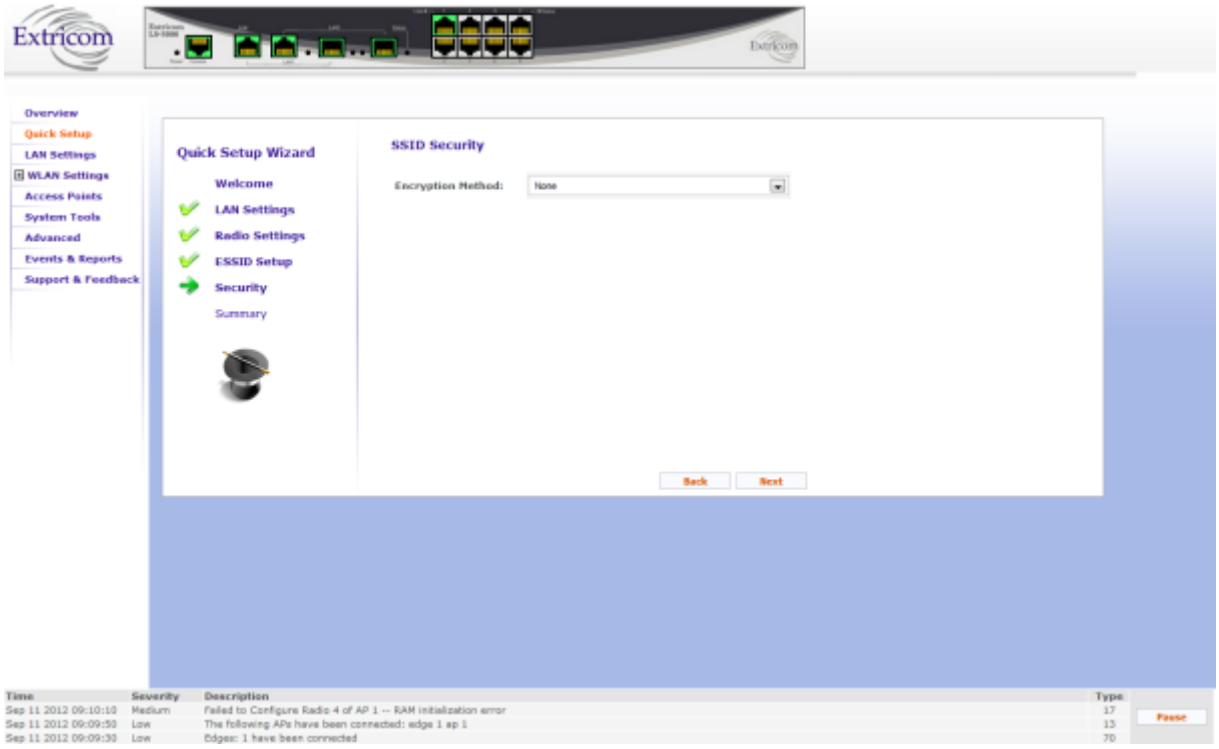


Figure 68: The SSID Security window

9. Select the Encryption Method.
10. Click **Next**. The **Summary** window appears.

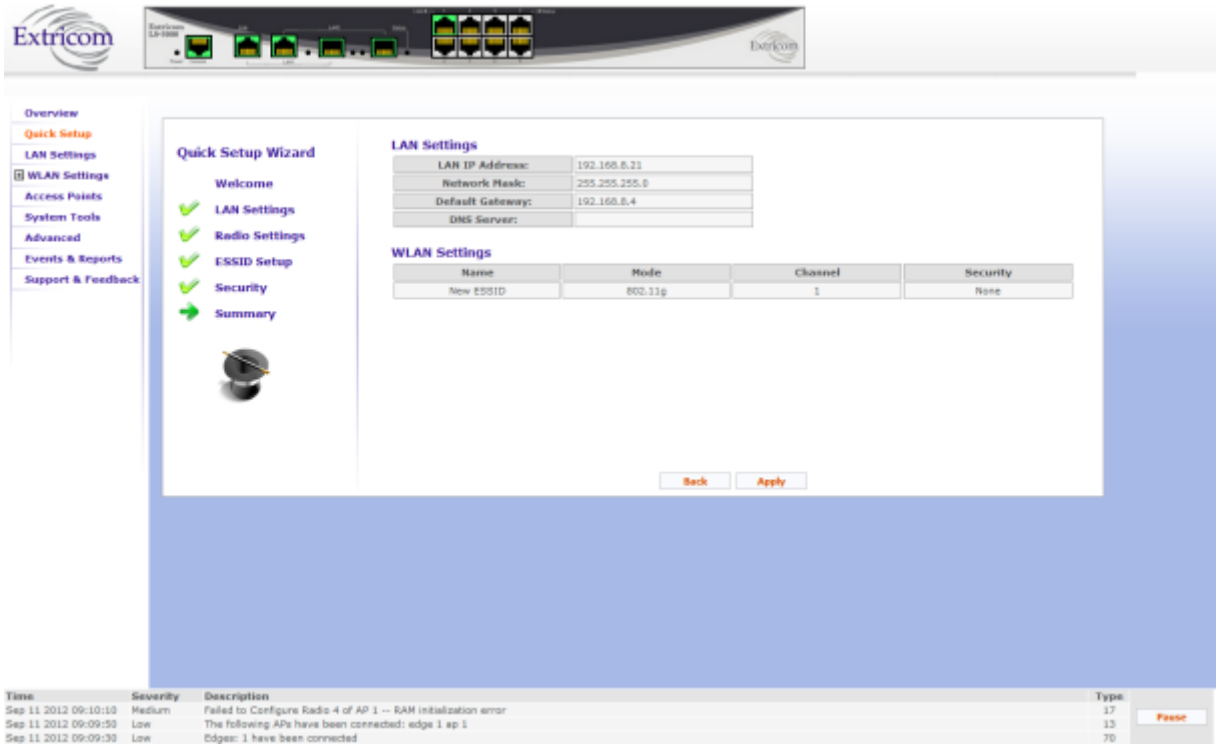


Figure 69: The Summary window

11. Review the settings to make sure that they are correct. Click **Apply** to configure the switch according to the settings that you chose and exit the Quick Setup Wizard.

IMPORTANT! Using the Quick Setup Wizard will overwrite any existing LAN and WLAN settings. You may wish to save your current configuration data to the disk.

Configuring LAN Parameters

In the *LAN Configuration* page, you can configure the following:

- The LAN port's IP address along with the network mask, as well as a backup IP address with its network mask.
- The LAN interface and management VLAN tag IDs.
- The default gateway.

To configure LAN parameters:

- Click **LAN Settings** in the navigation tree. The *LAN Settings* page appears (refer to Figure 20).
- Configure the LAN parameters. Refer to Table 6 for a description of the LAN parameters. Refer to Table 30 for the fields that have been added to or removed from the LS-3000 switch.

Field	Description
Force SFP 1000-Full Duplex	A switch to set the LAN for a full duplex fiber optical connection.
Link Aggregation	Does not appear in the LS-3000 switch

Table 30: LAN Configuration Parameters Differences

- Click **Save** to save the configuration.

IMPORTANT! The changes made to the configuration will be lost, if you do not click **Apply** in the **System Tool**s configuration section after clicking **Save** on one or several configuration pages. Please refer to the Reboot section.

Configuring WLAN Settings

The *WLAN Settings* section is subdivided into three menu sub-sections:

- ESSID Definition
- Radios
- Assignments

Configuring ESSID Definition

For more information, refer to **Error! Reference source not found.** on page **Error! Bookmark not defined.**

ESSID Settings

The following table contains the differences in the ESSID parameters for the LS-3000 switch.

Field	Description
Multicast Rate Control	Removed
Broadcast Rate Control	Removed

Table 31: ESSID Parameter Descriptions Differences

The following table contains the differences in the Security parameters, also displayed on the ESSID window.

Field	Description
RADIUS Authentication Servers	Removed
RADIUS Accounting Server	Select the RADIUS accounting server from the drop-down list of RADIUS servers.

Table 32: Security Parameter Descriptions Differences

Configuring WLAN Radios

Configuring Radios Manually

To configure each radio manually, click on the *Radios* tab to get to the Radios configuration screen.

When the Radios page is initially displayed, it appears in its abridged form. To see all of the configuration options, you must click on the “More Options” button. The window as shown in Figure 27 appears.

Note that when configuring 802.11a/b/g radios, the 802.11n displayed parameters cannot be configured and are grayed out.

The configuration parameters of each radio are arranged in a column. There are four columns, each of which is clearly identified with the corresponding title, i.e. **Radio 1**, **Radio 2**, etc. Refer to the Table 15 to set up the configuration parameters. Refer to Table 33 for the differences in the parameters for the LS-3000 switch.

Field	Description
Channel Options	
Select Country	Select the country. The particular country can have an effect on the channel selection.
Enable TrueReuse	Removed

Table 33: Radio Configuration Parameters

Powering EDGE Switches

The Edge switches are independently-powered and do not use PoE. The PoE output from the LS-3000 unit provides the power for the EXMC-1000 Media Converters, which provide a fiber optical connection between the LS-3000 and the MS-1000 switches.

The Access Points are powered via PoE from the Edge switches.

Click on *Access Points* in the navigation tree. Under *PoE & Radio Controls* tab:

- Toggle an individual Edge PoE on or off by clicking on its RJ45 connector image. The RJ45 connector image will turn either green or grey depending on whether it has been powered on or off respectively. To immediately activate your selection, click the **Apply** button on the right side of the configuration screen.
- An image of an MS-1000 switch connected to the RJ45 connector will appear if an Edge switch is powered-on and connected to the port.
- To power on all of the Edge Switches with PoE, click the **Power on all** button on the right side of the screen.
- To power off all of the APs with PoE, click the **Power off all** button on the right side of the screen.

> Note: the image of the switch on top of the page also color illustrates the PoE status of the APs.

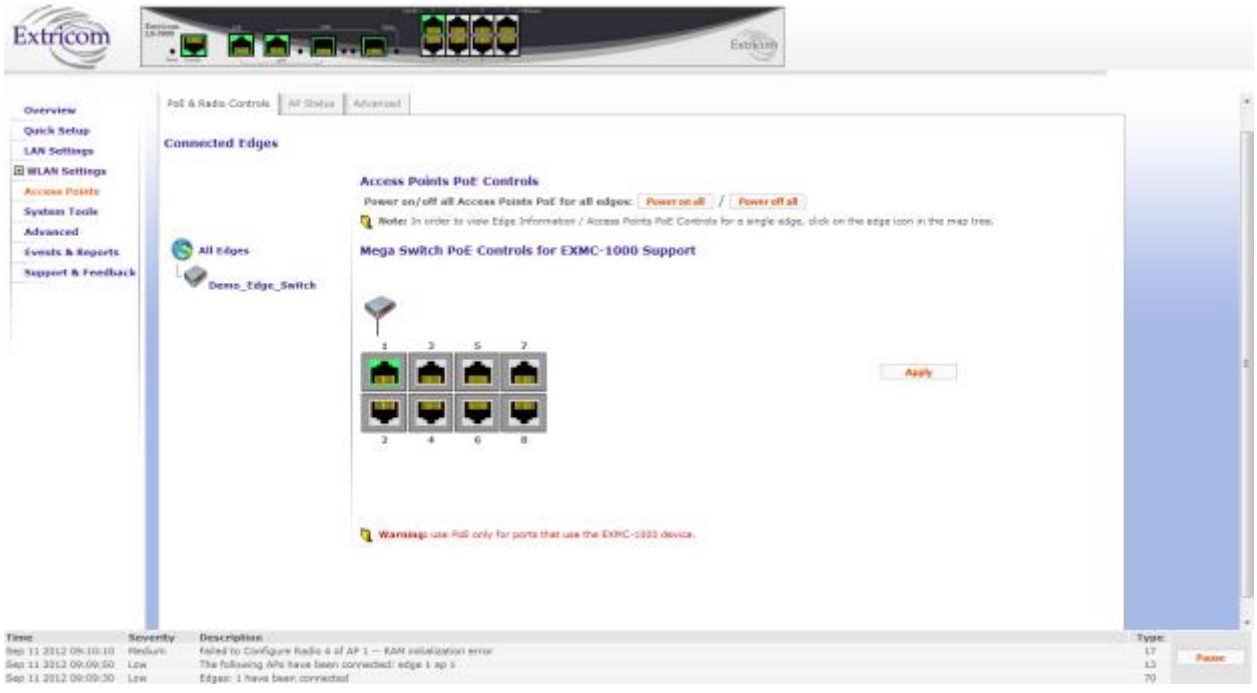


Figure 70: Access Points PoE & Radio Controls Page

To see which ports of the AP are up or down, click on the *AP Status* tab. To display the most up-to-date information, click on the **Refresh** button on the right.

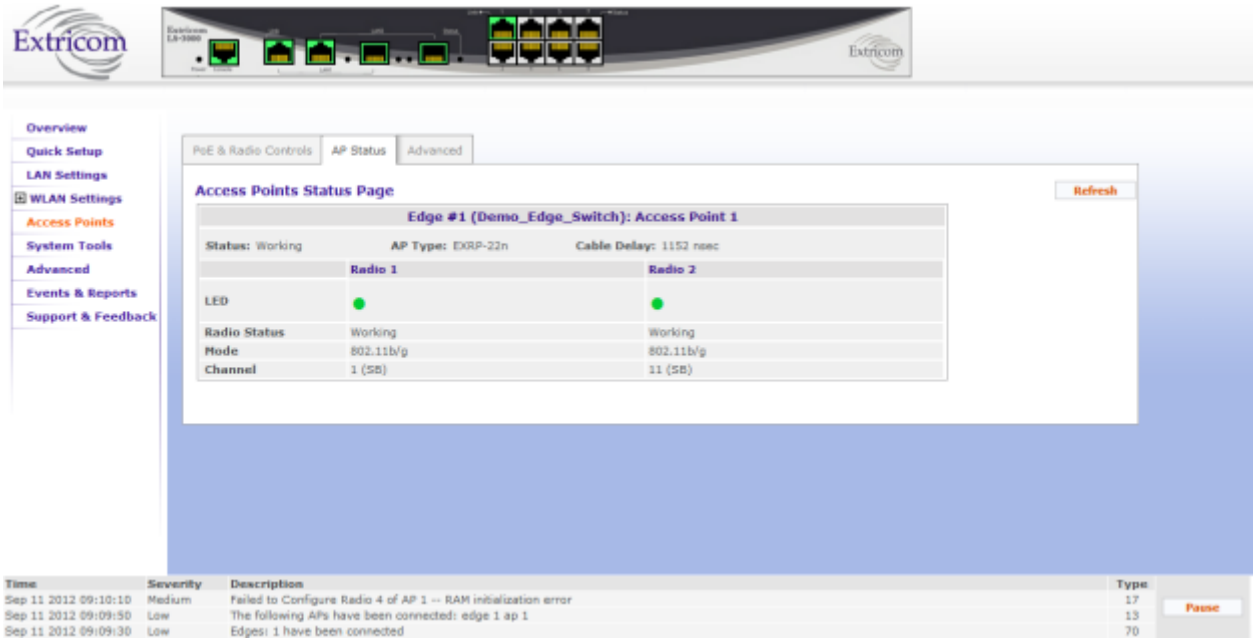


Figure 71: Access Points Status Page

To activate the Access Point LEDs, click on the *Advanced* tab.

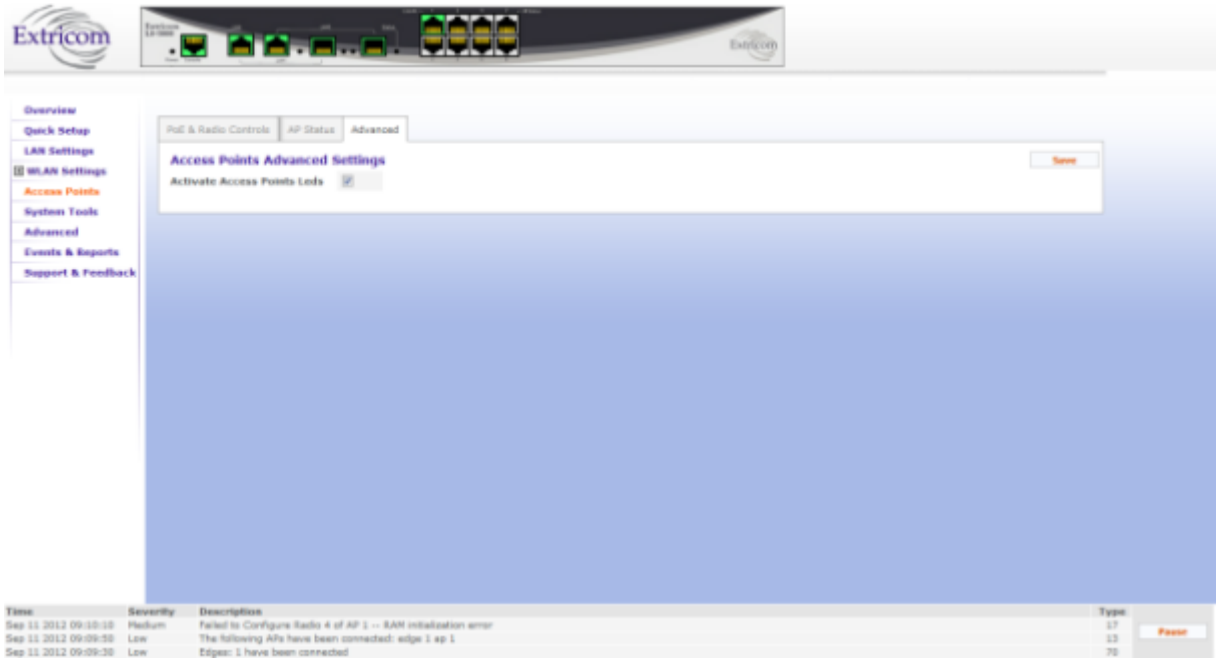


Figure 72: Access Points Advanced Settings Page

System Tools Configuration

For information on configuring the system tools, refer to System Tools Configuration on page 64.

Advanced Configuration – LS-3000 Differences

To configure advanced features, select **Advanced** from the navigation tree. For more detailed information, refer to Advanced Configuration on page 75.

Redundancy

1. Switch redundancy refers to redundancy over wired LAN media and provides the master-to-backup auto fallback functionality. Both switches serve a single BSSID until either of them is at fault. As soon as one of the switches fails, the surviving switch serves mobile devices by itself with no human intervention. The eventual replacement of the faulty switch does not necessitate any interruption in service, while returning to a fully redundant mode.

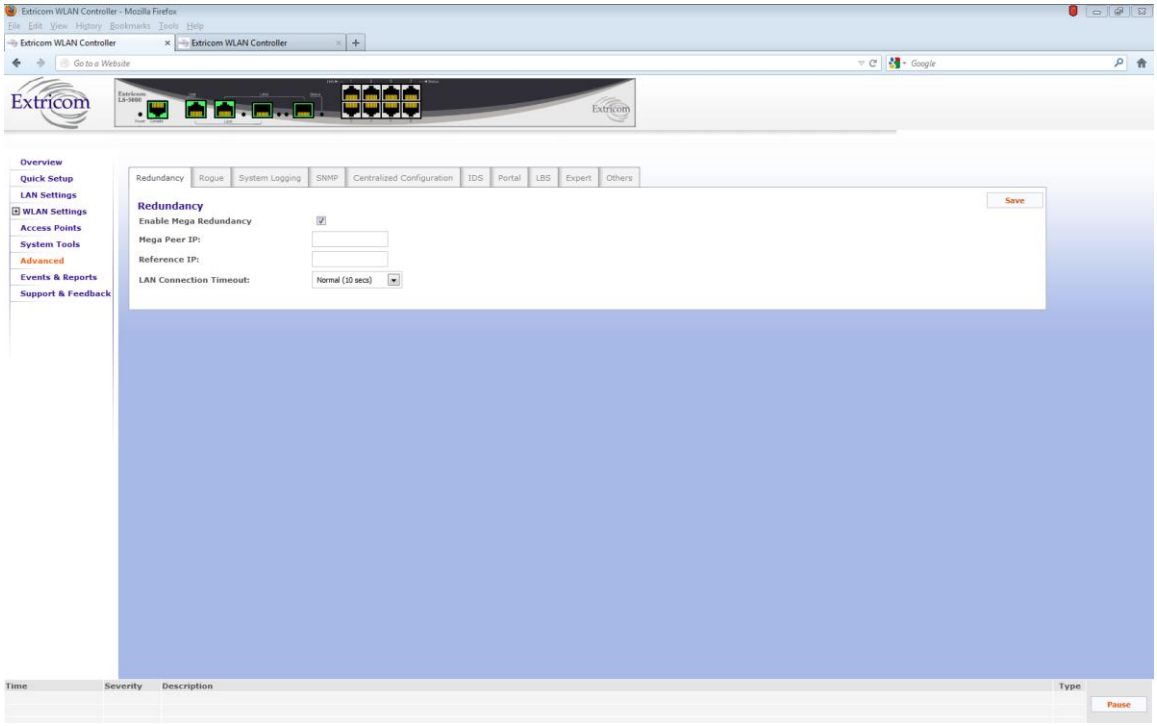


Figure 73: Redundancy Configuration Tab

> **!** Redundancy is only available if an appropriate license is installed. To check whether redundancy has been installed, refer to License on page 72. If it is not available, refer to your Extricom distributor.

Redundancy Fields for Primary Switch

Table 34 lists all available options under the *Redundancy* configuration screen fields.

Field	Description
Enable Mega Redundancy	Select this field to enable redundancy.
Mega Peer IP	IP address of the LS-3000 device on the LAN.
Reference IP	IP address of a reference device on the LAN. This is used to test connectivity to the LAN. The reference device must be operational and respond to pings.
LAN Connection Timeout	Interval in seconds before a timeout state occurs. The default is 10 seconds.

Table 34: Redundancy Configuration Tab Parameters for a Primary Cascade Switch

Once the changes are made, you must click Save, then go to System Tools and apply changes as described in the Apply section, in order for them to take effect.

When a switch failure or a link failure has been detected, a failover occurs and the switch that remains fully operational goes into standalone mode.

> **!** Once the fault that caused the switchover has been resolved, both switches must be rebooted in order for them to return to normal cascade operation. Otherwise, they will continue to operate in standalone mode.

Multicast

This option is not available for the LS-3000 switches.

Viewing Events and Reports

The *Events & Reports* page provides performance reports and lists various system events. To access this page click **Events & Reports** in the navigation tree. For more information, refer to Viewing Events and Reports on page 95.

> **!** Diagnostics reports are not available for the LS-3000 switch.

Overview of the Configuration

The *Overview* page provides a summary of the current configuration. To get to it, click **Overview** in the navigation tree.

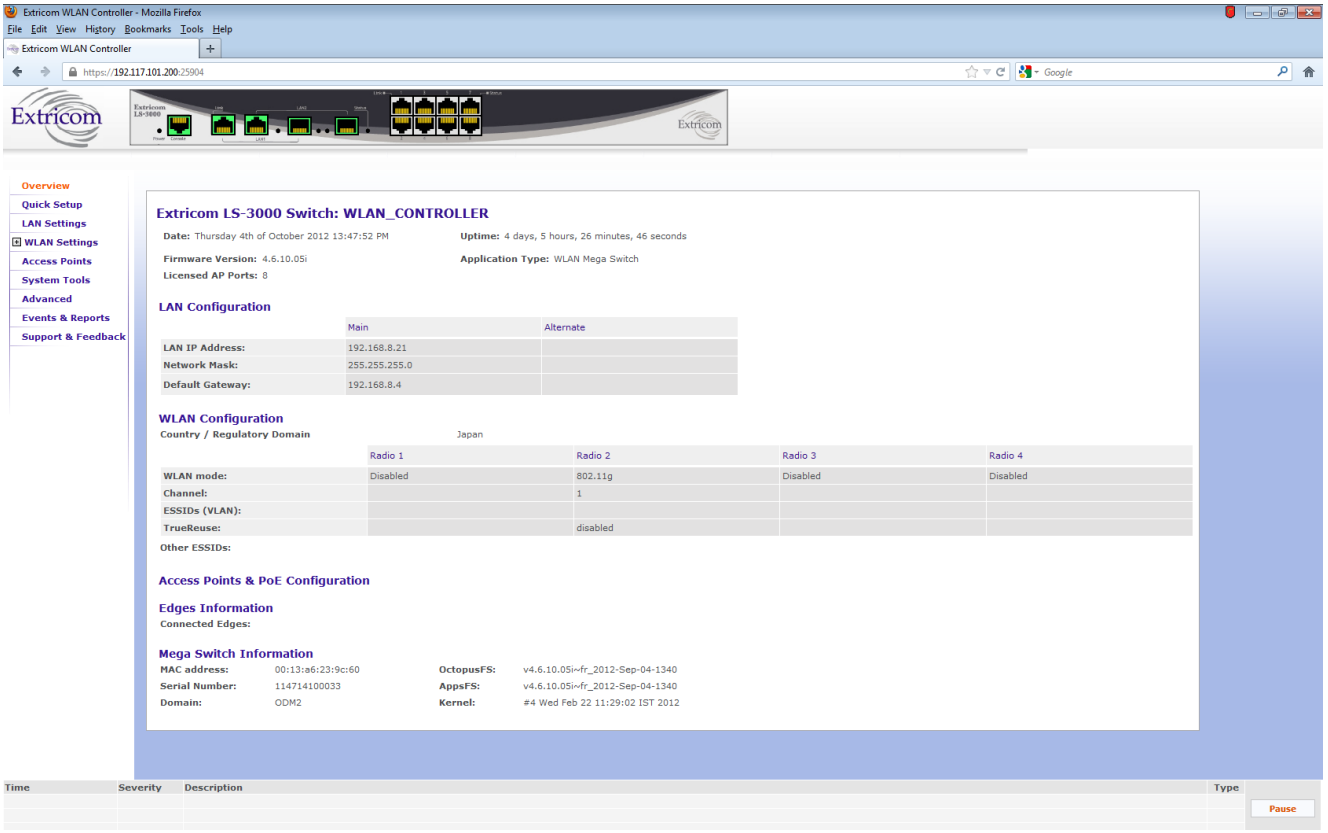


Figure 74: Configuration Overview of LS-3000

Field	Description
Date	Displays the date and time the summary was created.
Uptime	Displays the amount of time the switch has been up since the last reboot.
Firmware Version	Displays the firmware version installed on the switch.
Application Type	Displays the application type of the main switch.
Licensed AP Ports	Displays the number of ports that can be utilized for Edge switches.
LAN Configuration	
Main	IP address of the switch.
	Network mask.
	The IP address of the default gateway.

WLAN Configuration	
Country/Regulatory Domain	Displays the regulatory domain name currently in use by the switch.
WLAN mode	Displays the WLAN mode for each radio. (Disabled, 802.11a, 802.11b, 802.11g, 802.11b/g, 802.11n/a, 802.11n/g, 802.11n/b/g, or Rogue).
Channel	Displays the channel for each radio.
ESSIDs (VLAN)	Displays the ESSIDs and their related VLANs, defined and assigned to each radio.
TrueReuse	Shows whether TrueReuse is enabled or disabled for each radio.
Other ESSIDs	Displays other ESSIDs that are defined but are not assigned to any specific radio.
Access Points & PoE Configuration	
Edges information	Displays information regarding the connected Edge switches.
Mega Switch Information	
MAC address	Displays the base MAC address of the switch.
Serial Number	Displays a unique serial number of the switch.
Domain	RF localization indication.
OctopusFS:	Extricom firmware application version and build date.
AppsFS	Third-party software application version and build date.
Kernel	Extricom-specific Linux kernel build date.

Table 35: **Summary of the Overview Page**

Chapter 5

Troubleshooting

Table 36 lists problems you may encounter with your WLAN and provides possible solutions. If after trying the solutions you are still experiencing difficulties, contact Extricom Customer Support.

Problem	Solution
The AP Power LED is not lit.	• Verify that the AP Ethernet cable is connected to the switch and to the AP. The APs get PoE from the switch. • Verify that the AP is not turned off in the *Access Points* Web configuration page (refer to *page 124*).
A wireless device can't associate with a specific ESSID	• Verify that the wireless device supports the same 802.11 standard as configured for the ESSID (802.11/a/b/g). • Verify that the wireless device is set to connect to the specific ESSID. • Verify that the wireless device supports the security standard used by the ESSID, e.g., WEP. • Verify that the security settings are configured to use the same authentication method. • If the RADIUS Server is used, verify that the wireless device is registered and has the necessary authorization.
Cannot connect to the Extricom web configuration pages	• Verify that the switch is connected to the LAN. • Verify that the correct IP address is used.
Low data rates	• Verify that the switch was not mistakenly configured to use low data rates. • Verify that there is no additional cause of interference (e.g., an additional WLAN network in the same proximity using the same frequencies as the Extricom WLAN, or that there are no cordless phones using the same frequencies, or microwave oven interference).
Wireless devices disconnect in a specific location	• Verify that there is no additional cause of interference (e.g., an additional WLAN network in the same proximity using the same frequencies as the Extricom WLAN, or that there are no cordless phones using the same frequencies, or microwave oven interference). • Add an additional AP to cover the area. Plug another AP into the switch, or relocate an existing Access Point.

Problem	Solution
Cannot access the switch's Web configuration GUI	• Verify that the workstation on which the Web browser is running is connected to the same LAN as the switch. • Verify that the URL entered for the switch begins with `https`.

Table 36: Troubleshooting

Chapter 6

Northbound SNMP Traps

The table below lists and describes the SNMP Traps sent by the Extricom Switch over the northbound interface.

SNMP Traps will only be sent if enabled in the switch configuration. Furthermore, some traps will only be sent if a specific feature is configured (e.g. traps 28-30 will only be sent if Rogue AP Detection is configured on the switch).

All SNMP Traps are sent according to RFC 1157 SNMPv1.

Trap No.	Trap Name	Description	Version
1	Client Association	This trap is sent whenever a client successfully associates with the switch. The trap includes the client MAC address and AID as well as the BSSID and ESSID that the client is associated to.	4.1 or above
2	Client Disassociation	This trap is sent whenever a client disassociates from the switch. The trap includes the client MAC address and AID as well as the BSSID and ESSID that the client disassociated from. The disassociation reason code is also sent.	4.1 or above
4	EAPOL Key Error	A client attempted to associate using WPA but there was an error with the EAPOL key. The trap will detail which of the following errors occurred: the key does not exist, there is a timeout, the key does not match, or the cypher does not match.	4.1 or above

Trap No.	Trap Name	Description	Version
13	AP Connected	One or more APs has been connected to the switch (AP has been physically connected via Ethernet cable, or it was already connected and PoE has been enabled). Tthe AP number corresponds to the port number on the switch that the AP is connected to. Upon switch startup or reconfigure, this trap will be sent listing all the APs connected.	4.1 or above
14	AP Off	One of more APs has been disabled. The AP Ethernet cable has either been physically disconnected from the switch or PoE has been turned off. The AP number corresponds to the port number on the switch that the AP is connected to.	4.1 or above
19	Redundancy peer connection up	When using "Normal" (not "Cascade") redundancy, this switch has regained connectivity with the peer switch.	4.1 or above
20	Redundancy peer connection down	When using "Normal" (not "Cascade") redundancy, this switch has lost connectivity with the peer switch	4.1 or above
21	Redundancy keepalive connection up	When using "Normal" (not "Cascade") redundancy, the switch regained connectivity to the Reference IP.	4.1 or above
22	Redundancy keepalive connection down	When using "Normal" (not "Cascade") redundancy, the switch lost connectivity to the Reference IP.	4.1 or above
25	Redundancy status up	When using "Normal" (not "Cascade") redundancy, this switch has taken over the wireless responsibility. If the Secondary switch is issuing this trap it will have done so because it detected a failure in the primary switch. If the Primary switch is issuing this trap it means it has recovered from an error and is now resuming wireless	4.1 or above

Trap No.	Trap Name	Description	Version
		responsibility.	
26	Redundancy status down	When using "Normal" (not "Cascade") redundancy, this switch has relinquished wireless responsibility. If the Primary switch is issuing this trap it means it discovered an error (for example connectivity to Reference IP is lost) in which case the trap will specify what the error is. If the Secondary switch is issuing this trap it means that the Primary has recovered from an error and the secondary is transferring wireless responsibility back to it.	4.1 or above
28	Rogue AP lost	Available only when Rogue AP Detection is enabled. This trap indicates that a previously discovered rogue network has stopped transmitting. The trap will detail if the rogue network was an AP or ad-hoc, the relevant BSSID and ESSID, what channel the rogue was transmitting on, which Extricom AP on the switch was closest to the rogue AP, and approximately how far the rogue AP was, from the Extricom AP.	4.1 or above
29	Rogue AP found	Available only when Rogue AP Detection is enabled. This trap indicates that a rogue network has been detected. The trap will detail if the rogue network is an AP or ad-hoc, the relevant BSSID and ESSID, what channel the rogue is transmitting on, which Extricom AP is closest to the rogue AP, and approximately how far the rogue AP is from the Extricom AP.	4.1 or above

Trap No.	Trap Name	Description	Version
30	Rogue AP update	Available only when Rogue AP Detection is enabled. This trap indicates that the status of a rogue AP has been updated. This trap will always come after trap 29. This trap will detail if the rogue network is an AP or ad-hoc, the relevant BSSID and ESSID, what channel the rogue is transmitting on, which Extricom AP is closest to the rogue AP, and approximately how far the rogue AP is from the Extricom AP.	4.1 or above
43	Intrusion detection Duration attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a Duration attack. The trap will detail the duration length as well as the transmitting MAC address.	4.1 or above
44	Intrusion detection Association Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an Association Flood attack. The trap will detail how many associations were received and within what time interval.	4.1 or above
45	Intrusion detection Disassociation Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a Disassociation Flood attack. The trap will detail how many disassociations were received and within what time interval. If the event was triggered from a per station limitation, the trap will also include the client MAC address.	4.1 or above
46	Intrusion detection Authentication Failure attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an Authentication Flood attack. The trap will detail how many associations were received and in what time interval.	4.1 or above

Trap No.	Trap Name	Description	Version
48	Intrusion detection Authentication Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an Authentication Flood attack. The trap will detail how many authentications were received and in what time interval.	4.1 or above
49	Intrusion detection De-Authentication Flood attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a De-Authentication Flood attack. The trap will detail how many de-authentications were received and in what time interval. If the event was triggered from a per station limitation the trap will also include the client MAC address.	4.1 or above
50	Intrusion detection RF Jamming attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an RF Jamming attack	4.1 or above
51	Intrusion detection EAPOL Start attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an EAPOL Start Flood attack. The trap will detail how many EAPOL Start packets were received and in what time interval. If the event was triggered from a per station limitation, the trap will also include the client MAC address.	4.1 or above
52	Intrusion detection EAPOL Logoff attack	Available only when Intrusion Detection is enabled. Indicates that the switch has detected an EAPOL Logoff Flood attack. The trap will detail how many EAPOL Logoff packets were received and in what time interval. If the event was triggered from a per station limitation, the trap will also include the client MAC address.	4.1 or above
53	Intrusion detection De-Authentication	Available only when Intrusion Detection is enabled. Indicates that the switch has detected a De-	4.1 or above

Trap No.	Trap Name	Description	Version
	Broadcast	Authentication Broadcast	
54	Radius Timeout	A client attempted to associate to an ESSID using 802.1x authentication. A timeout was reached when attempting to contact the RADIUS server. If the ESSID has a secondary RADIUS server configured, the switch will attempt to authenticate the client using this server. The trap details which ESSID the authentication attempt occurred on.	4.1 or above
55	Radius Changed selection	This trap will occur after trap 54, if the ESSID has multiple RADIUS servers configured. The trap will detail which RADIUS server it is changing from and to which server it is changing to.	4.1 or above
56	Last Radius Failed	This trap will occur after traps 54 and 55. If the switch was unable to contact all RADIUS servers, it will try again from the beginning of the RADIUS server list.	4.1 or above
57	RF localization failed	The switch localization lock is missing or corrupt. Contact an Extricom representative.	4.1 or above
59	Firmware upgrade startup	Switch firmware upgrade has started.	4.2.42.2 or above
60	Firmware upgrade done	Switch firmware upgrade has ended.	4.2.42.2 or above
61	Firmware upgrade progress	This trap is sent with a progress update during the switch firmware upgrade.	4.2.42.2 or above
62	Firmware upgrade failed	Switch firmware upgrade has failed.	4.2.42.2 or above

Trap No.	Trap Name	Description	Version
63	Reconfigure ended	Switch reconfigure has ended.	4.2.42.2 or above
65	Radio is not functioning in access points	One or more of the radios in a channel blanket is not functioning. The trap will detail which radio in which AP is not functioning.	4.1 or above
66	Radio is functioning normally in all access points.	All radios in a channel blanket are now functioning normally. Will be sent after all of the errors causing trap number 65 have been fixed.	4.1 or above
67	Client Ignore MTU	The client has been sending packets that are larger than the Switch MTU, even though the Switch has sent several adjust MTU packets to the client.	4.2.42.2 or above
68	Edge Mode Switchover	The secondary switch in a switch cascade is changing to standalone mode. This trap will be sent from the secondary switch. The trap will detail the reason for the switchover.	4.2.42.2 or above
69	Reconfigure started	Switch reconfigure has started.	4.2.42.2 or above
70	Edge Connected	A secondary switch of a switch cascade has connected and synchronized with the primary switch. This trap will be sent from the primary switch.	4.2.42.2 or above
71	Edge Disconnected	A secondary switch of a cascade has been disconnected from the primary switch. This trap will be sent from the primary switch. This trap will be sent if the link between the primary switch and the secondary is down or if the secondary switch is non-responsive	4.2.42.2 or above

Trap No.	Trap Name	Description	Version
72	Set Client IP	The Client now has an IP address set. The trap details the client MAC address, AID and the IP address it is set to use. The IP address was either received via DHCP or statically set and is being used by the client.	4.1 or above
73	Start.sh Started	Start.sh is being run on the switch.	4.2.42.2 or above
74	Start.sh ended	Start.sh has finished running on the switch.	4.2.42.2 or above
75	Starting Boot	the Switch is being rebooted.	4.2.42.2 or above
76	Changed Wireless Status (On/Off)	The wireless has been enabled or disabled on the switch. The trap will say if the wireless has been turned "ON" of "OFF" and will include the reason for the change. In case the wireless was turned "OFF", all radio LEDs on the APs will be constant RED. The wireless on a switch can be turned "OFF" or "ON" manually or automatically in case of a switch cascade redundancy event.	4.2.42.2 or above
77	Radio reset	A problem at the radio required a warm reset. The trap details which radio in which AP required the warm reset.	4.1 or above
78	AP reset	A radio required multiple warm resets and was still not working properly, so the whole AP was reset. The trap details which AP was reset.	4.1 or above
79	POE reset	An AP was reset but is still not working properly. The AP was power booted via PoE. The trap details which AP was PoE reset.	4.1 or above

Table 33: SNMP Traps

Appendix A

Internal Access Point Mounting Template

4.25 inches

10.8 cm.

Important Note: Due to variations in printers, when printing this page, printer Page Scaling should be set to “None” or diagram may be automatically reduced in size. As double-check, make sure distance between drill points is as indicated above.